VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belgaum -590014, Karnataka.

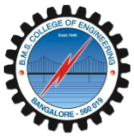
LAB REPORT
on

Ethical Hacking

Submitted by

Rajdeep Bandyopadhaya (1BM22IC045)

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING(IoT and Cybersecurity including Blockchain)



B.M.S. COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019
March-2025 to June-2025

B. M. S. College of Engineering,

Bull Temple Road, Bangalore 560019

(Affiliated To Visvesvaraya Technological University, Belgaum)

Department of Computer Science and Engineering(IoT and Cybersecurity including Blockchain)

CERTIFICATE

This is to certify that the Lab work entitled "Ethical Hacking" carried out by **Rajdeep Bandyopadhaya (1BM22IC045),** who is a bonafide student of **B. M. S. College of Engineering.** It is in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering(IoT and Cybersecurity including Blockchain)** of the Visvesvaraya Technological University, Belgaum during the year 2025. The Lab report has been approved as it satisfies the academic requirements in respect of a **Ethical Hacking (23IC6PCEHG)** work prescribed for the said degree.

Krupa K S
Assistant Professor
Department of CSE(ICB)
BMSCE, Bengaluru

Dr. Prasad G R
Professor and Head
Department of CSE(ICB)
BMSCE, Bengaluru

Index Sheet

Ethical Hacking Report – 01 (Date: 22-03-2025)

Ethical Hacking Fundamentals

EC-Council Lab Assignment: Module 2

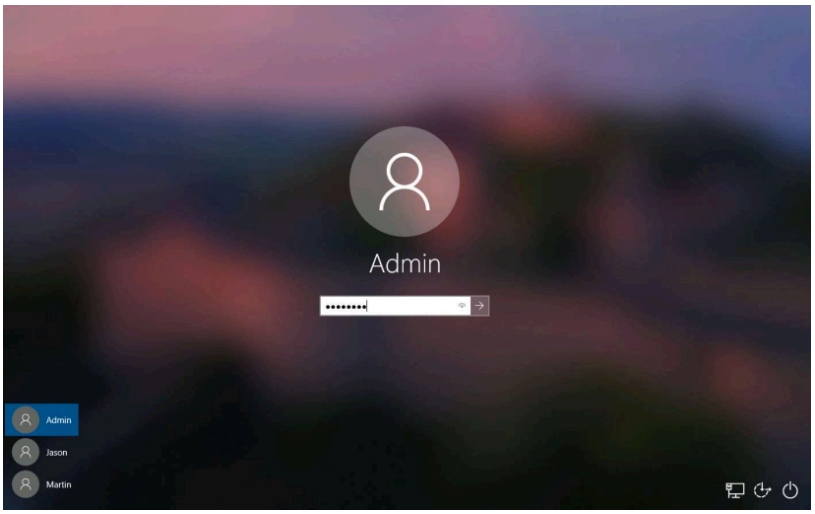
Perform passive footprinting to gather information about a target

Ethical hackers or pen testers use numerous tools and techniques to collect information about the target. Here we learned various footprinting techniques include:

1. Gather information using advanced google hacking technique

1.1. First select the Windows 10 machine and press **Ctrl+Alt+Delete** (or use the button in the Resources pane or Commands menu).

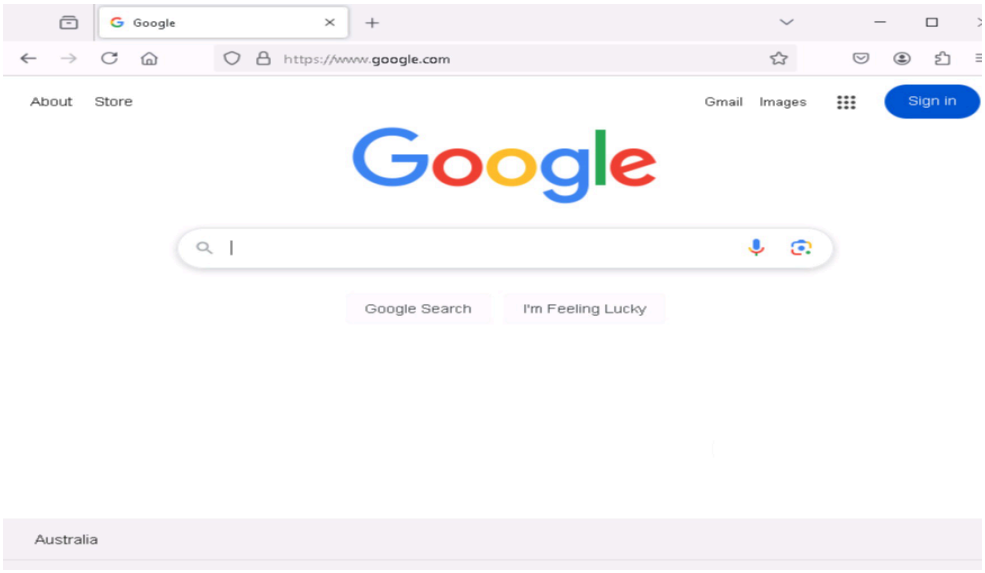
1.2. Click **Pa$$w0rd** to paste it in the Password field and press **Enter** to log in.



1.3. If the **Welcome to Windows** wizard appears, click **Continue**, then click **Cancel** in the **Sign in with Microsoft** wizard.

1.4. On the **Networks** screen, click **Yes** to allow network discovery.

1.5. Open **Mozilla Firefox**, type https://www.google.com in the address bar, and press **Enter**.



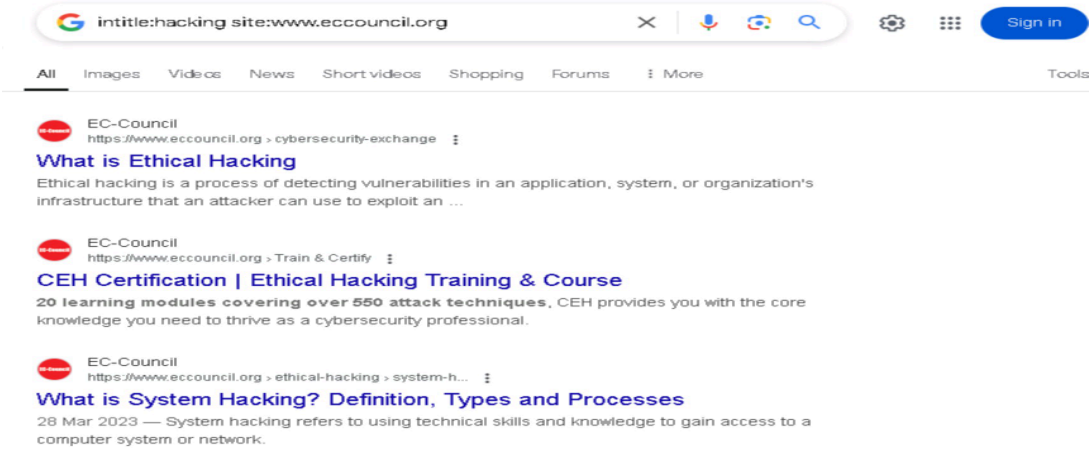
1.6. If a **Default Browser** pop-up appears, uncheck the checkbox and click **Not now**.

1.7. If a **Content Blocking** pop-up appears, click **Got it**.

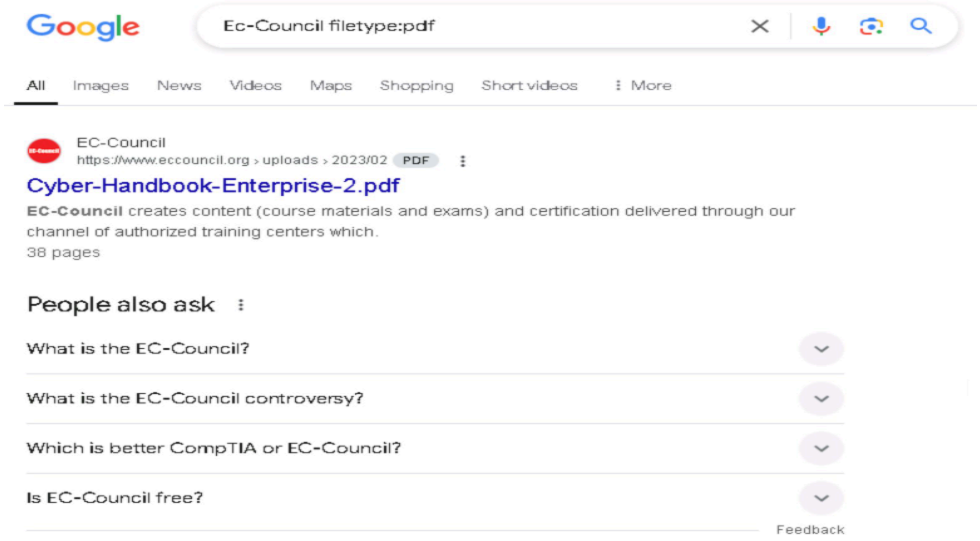
1.8. If a **notification** appears at the top, click **Okay, Got it**, then click **I agree** in the Google Search wizard.

1.9. When Google search appears, dismiss any pop-ups by clicking **No, thanks**.

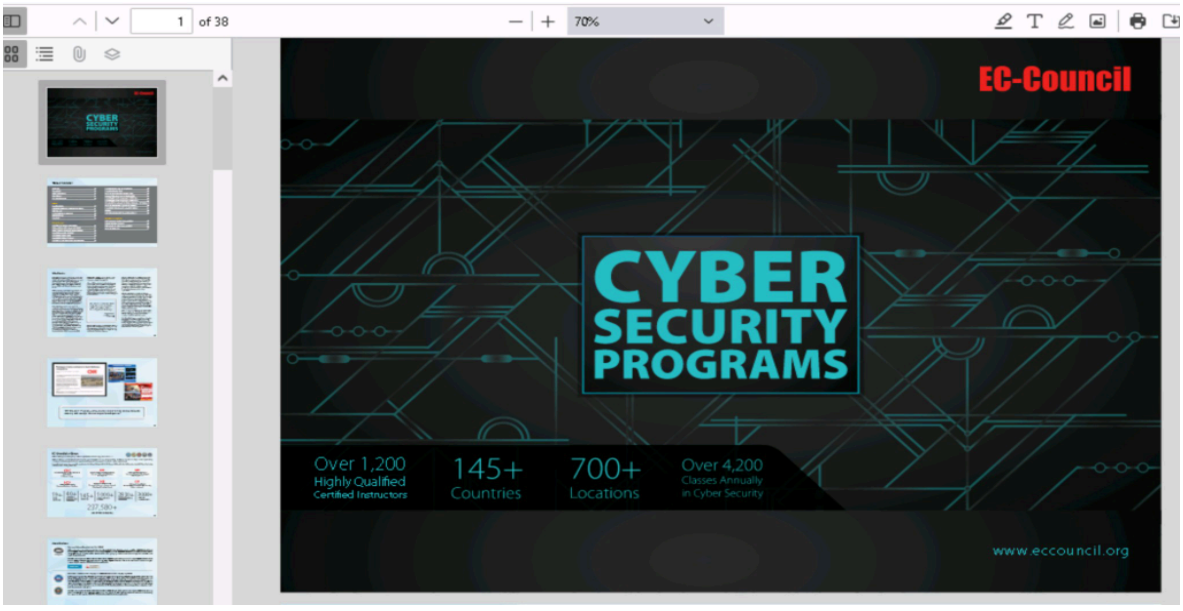
1.10. Use filter **intitle:hacking site:www.eccouncil.org** in a search command The query will show results only from the **EC-Council** website where the word **"hacking"** appears in the title.



1.11. Use the filter **EC-Council filetype:pdf** is a search command.The query will show PDF files related to **EC-Council** in the search results.

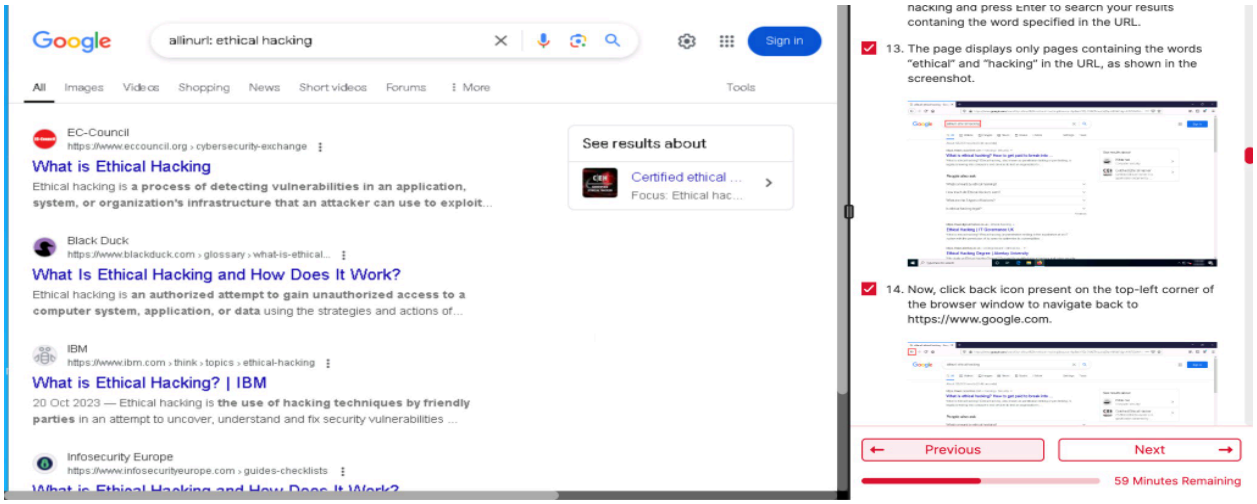


1.12. Now, click on any link from the results



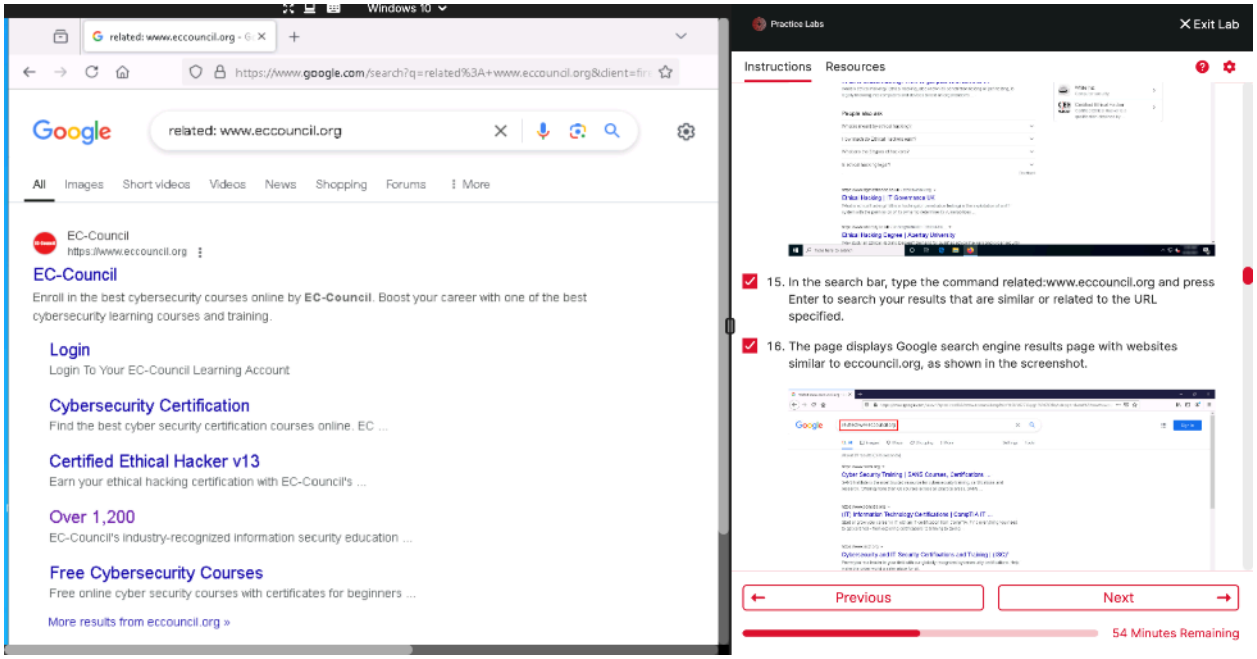
This will appear displaying the PDF file, as shown in the screenshot.

1.13. In the search bar, type the command **allinurl: ethical hacking** and press **Enter** to search your results containing the word specified in the URL.



The page displays only pages containing the words “ethical” and “hacking” in the URL, as shown in the screenshot.

1.14. Now go back and filter **related:www.eccouncil.org** is a search command used in search engines.
The query will show websites that are similar or related to **EC-Council's** website.



17. Apart from the aforementioned advanced Google operators, you can also use the following to perform an advanced search to gather more information about the target organization from publicly available sources.
    - cache: This operator allows you to view cached version of the web page. [cache:www.google.com]- Query returns the cached version of the website www.google.com
    - inurl: This operator restricts the results to pages containing the word specified in the URL [inurl: copy site:www.google.com]—Query returns only pages in Google site in which the URL has the word "copy"
    - allintitle: This operator restricts results to pages containing all the query terms specified in the title. [allintitle: detect malware]—Query returns only pages containing the words "detect" and "malware" in the title
    - inanchor: This operator restricts results to pages containing the query terms specified in the anchor text on links to the page. [Anti-virus inanchor:Norton]—Query returns only pages with anchor text on links to the pages containing the word "Norton" and the page containing the word "Anti-virus"
    - allinanchor: This operator restricts results to pages containing all query terms specified in the anchor text on links to the page. [allinanchor: best cloud service provider]—Query returns only pages in which the anchor text on links to the pages contain the words "best," "cloud," "service," and "provider"
    - link: This operator searches websites or pages that contain links to the specified website or page. [link:www.googleguide.com]—Finds pages that point to Google Guide's home page
    - info: This operator finds information for the specified web page. [info:gothotel.com]—Query provides information about the national hotel directory GotHotel.com home page
    - location: This operator finds information for a specific location. [location: 4 seasons restaurant]—Query give you results based around the term 4 seasons restaurant
18. This concludes the demonstration of gathering information using advanced Google hacking techniques. You can conduct a series of queries on your own by using these advanced Google operators and gather the relevant information about the target organization.
19. Close all open windows and document all the acquired information.

Question 2.1.1.1

Use an advanced Google hacking technique to find PDF files on the www.eccouncil.org website. Enter the complete URL of the Cyber-Handbook-Enterprise-2.pdf file.

https://www.eccouncil.org/wp-conte

Score

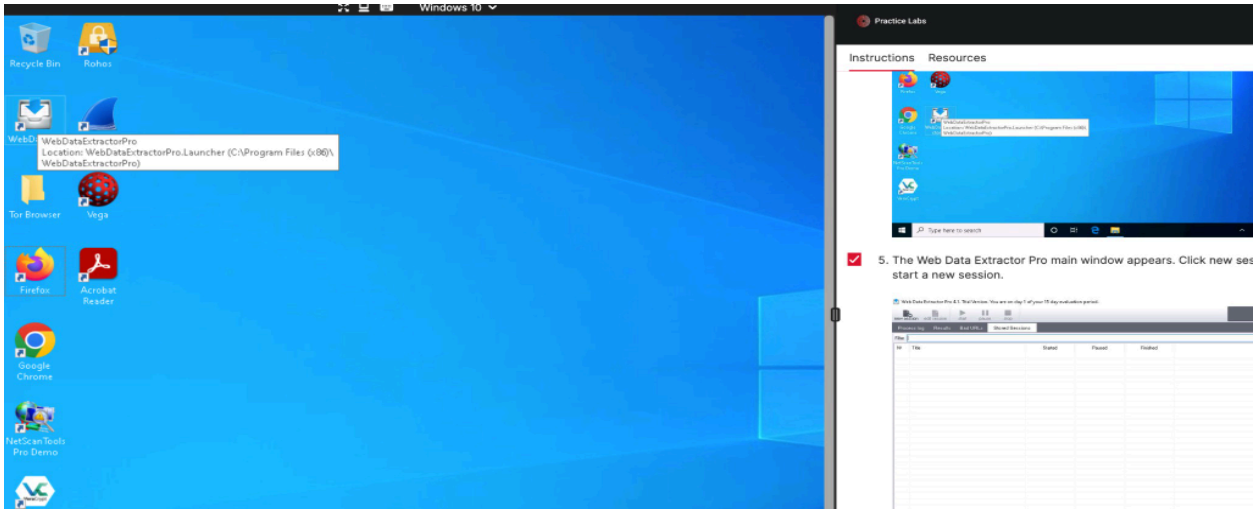
Correct

2. Extract a company's data using Web Data Extractor

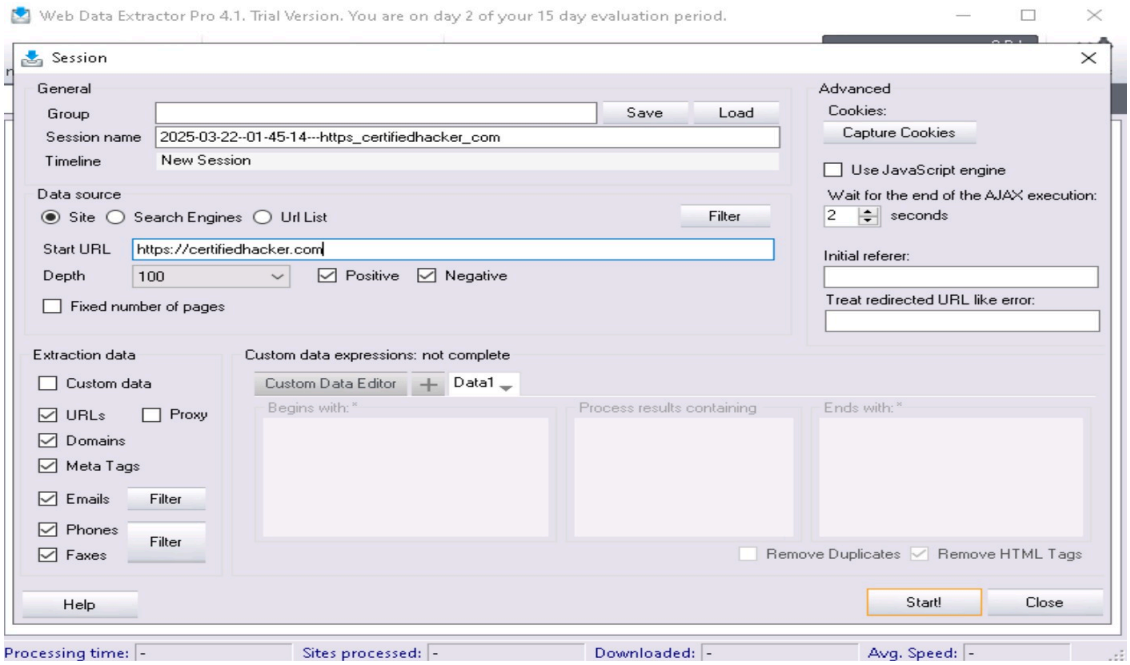
Web data extraction gathers information from a company's website, including contact details, URLs, and meta tags. Tools like **Web Data Extractor** use web spiders to automate data collection for ethical hacking.

2.1. Follow the wizard steps to install Web Data Extractor Pro and click **Finish**.

2.2. After installation, launch **Web Data Extractor Pro** from **Desktop**.

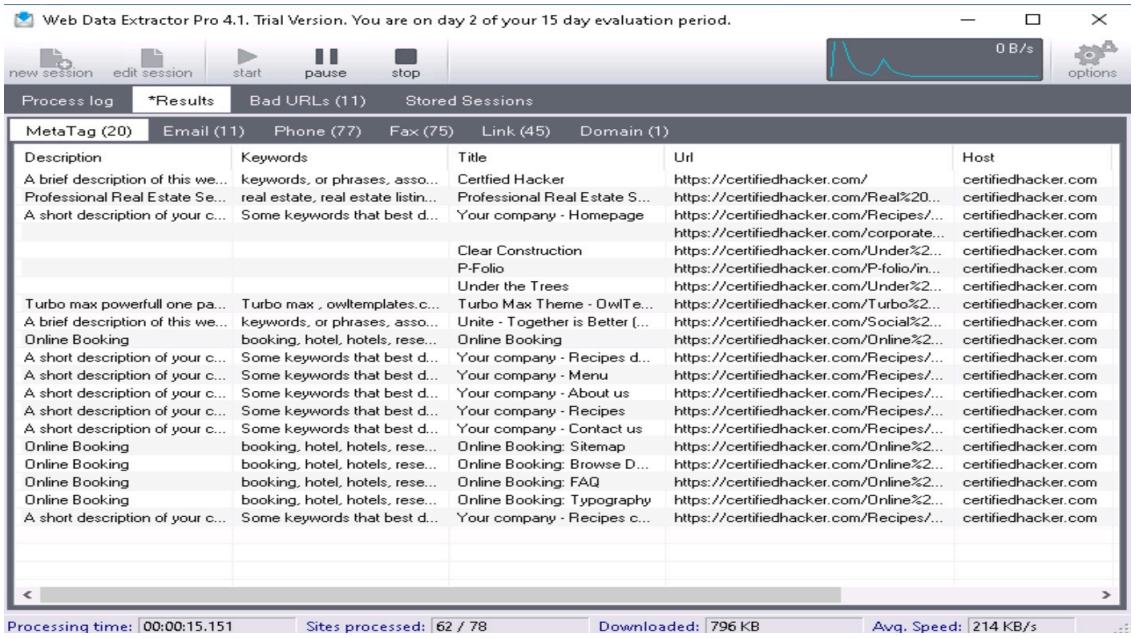


2.3. Lunch The **Web Data Extractor Pro** main window appears. Click **new session** to start a new session.



The **Session** window appears; type a URL (here, **https://www.certifiedhacker.com**) in the **Start URL** field. Check all the options, as shown in the screenshot and Click **Start** to initiate the data extraction.

2.4. Now click on **Results** tab to view the collected information about the website.



- Select the **Meta tag** tab to view details like URL, Title, Keywords, and Description.
- Select the **Email** tab to see email-related information.
- Select the **Phone** tab to check phone details.
- Explore the **Fax, Link, and Domain** tabs for more information.

2.5. This completes the demonstration of **Web Data Extractor Pro** for extracting company data.

Question 2.1.2.1

In the Windows 10 machine, use Web Data Extractor Pro web spidering tool located at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\Web Spiders\Web Data Extractor to gather the target company's data. Enter the target website that was used in this task to gather information.

https://www.certifiedhacker.com

Score

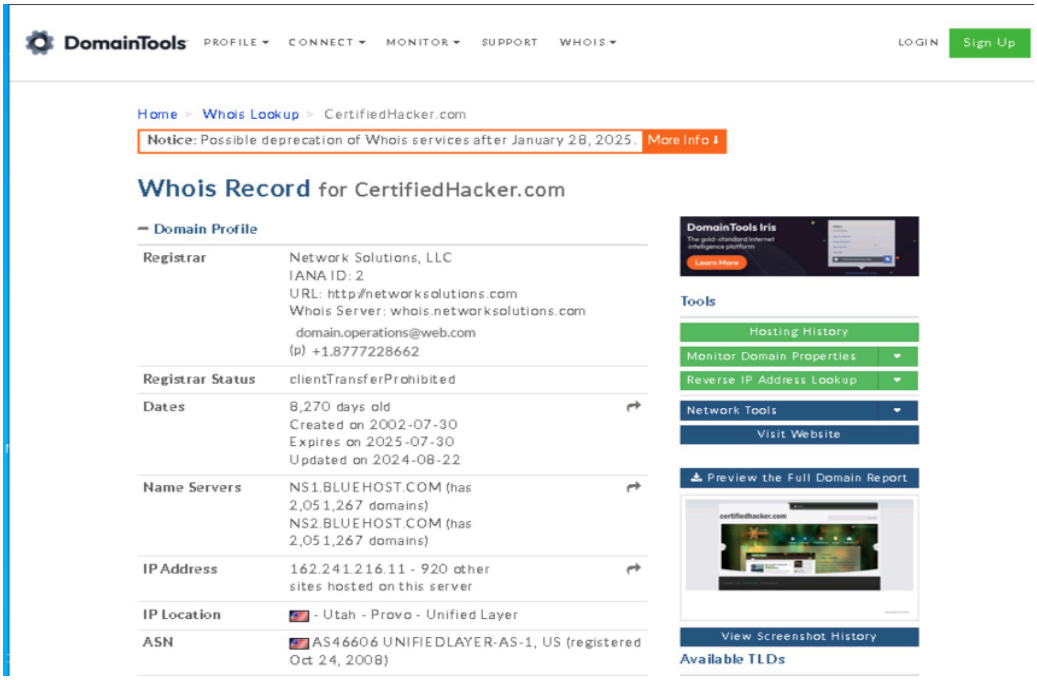
Correct

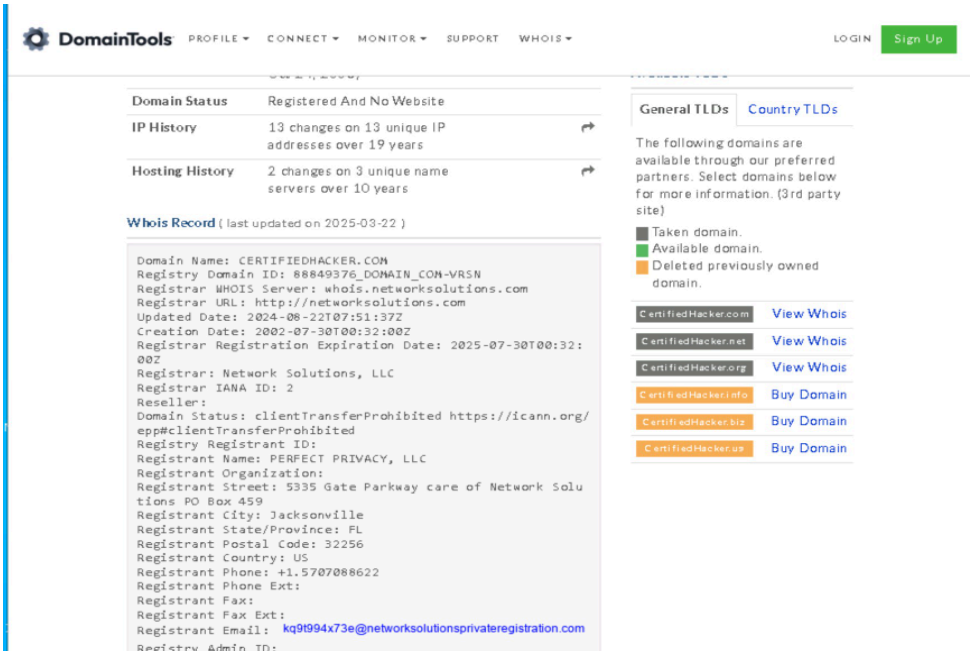
3. Perform whois lookup using DomainTools

Whois is a protocol used to query databases storing details of domain owners and IP addresses. It operates on port 43 (TCP) and is managed by Regional Internet Registries (RIRs). Whois databases provide information such as owner details, creation & expiration dates. DomainTools can be used to perform a Whois lookup to gather target information.

3.1. On the **Windows 10** machine, open a web browser (**Mozilla Firefox**). In the address bar, enter http://whois.domaintools.com and press **Enter** to open the **Whois Lookup** website

3.2. **Enter a domain or IP address...** search bar, type **www.certifiedhacker.com** and click **Search**.





This concludes the demonstration of gathering target organization information using Whois lookup on DomainTools.

Question 2.1.3.1

Perform Whois Lookup using DomainTools (http://whois.domaintools.com) and find the Registrant Postal Code of www.certifiedhacker.com website.

32256

Score

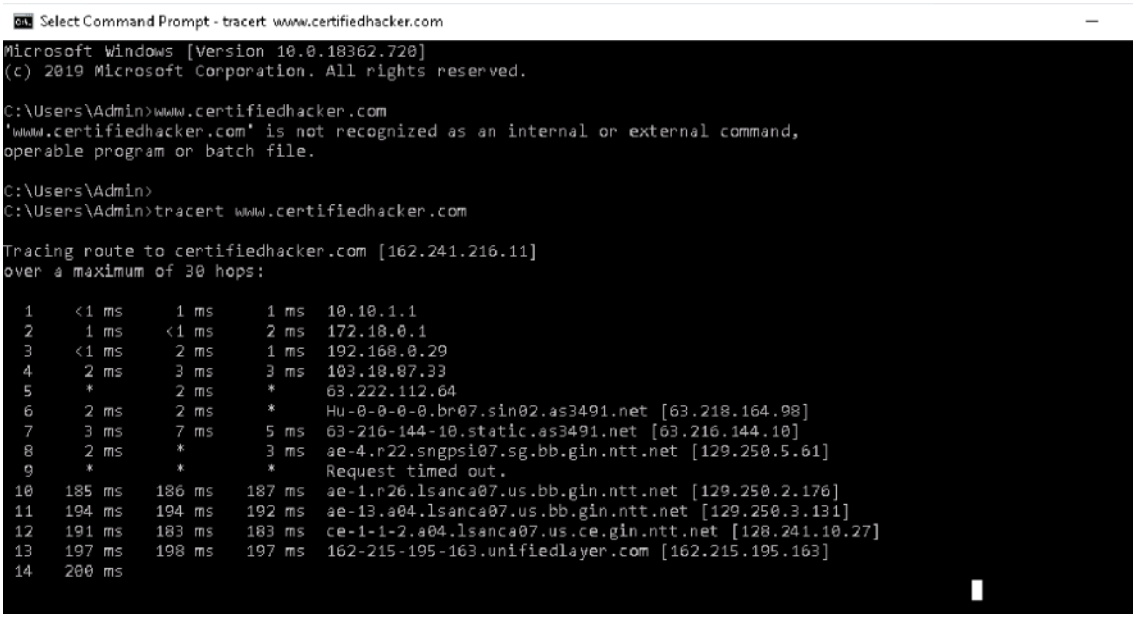
Correct

2. Perform network scanning to identify live hosts, open ports and services and target OS in the network

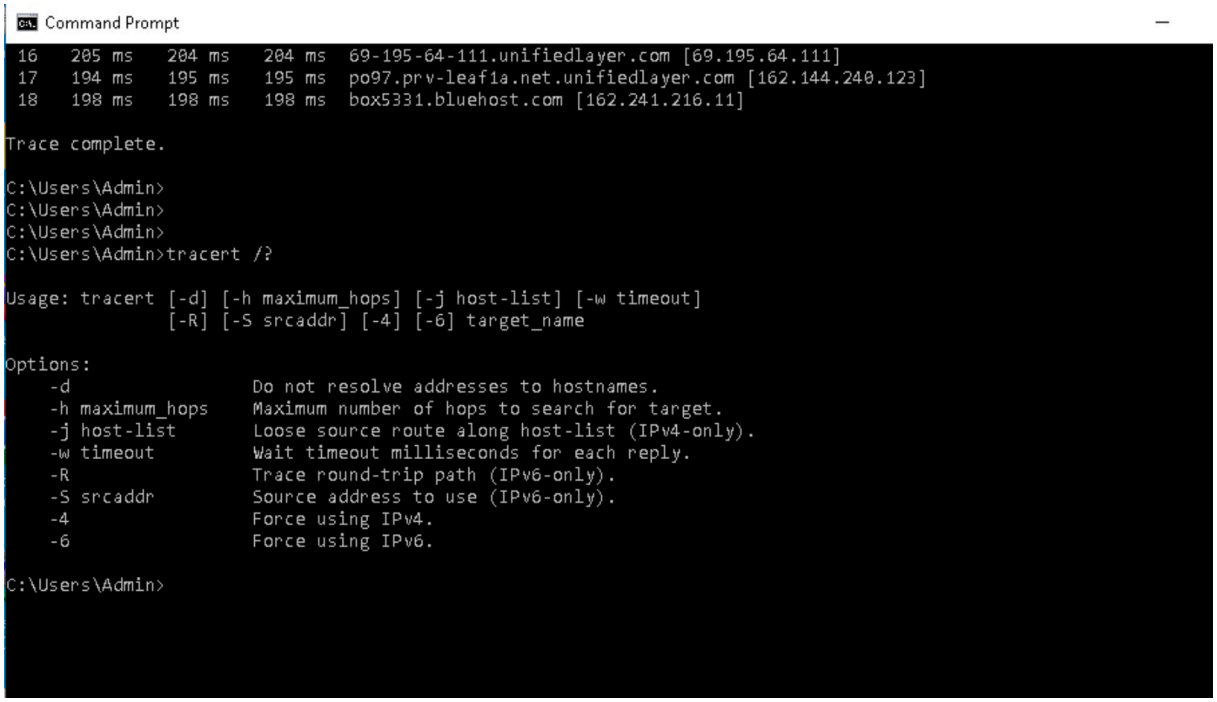
○ Perform network tracerouteing in Windows and Linux machines

Network tracerouting identifies the path a packet takes between the source and destination. It provides details like **IP addresses of intermediate hosts**, helping map **network topology**. Traceroute reveals **trusted routers, firewall locations, and network structure** of an organization.

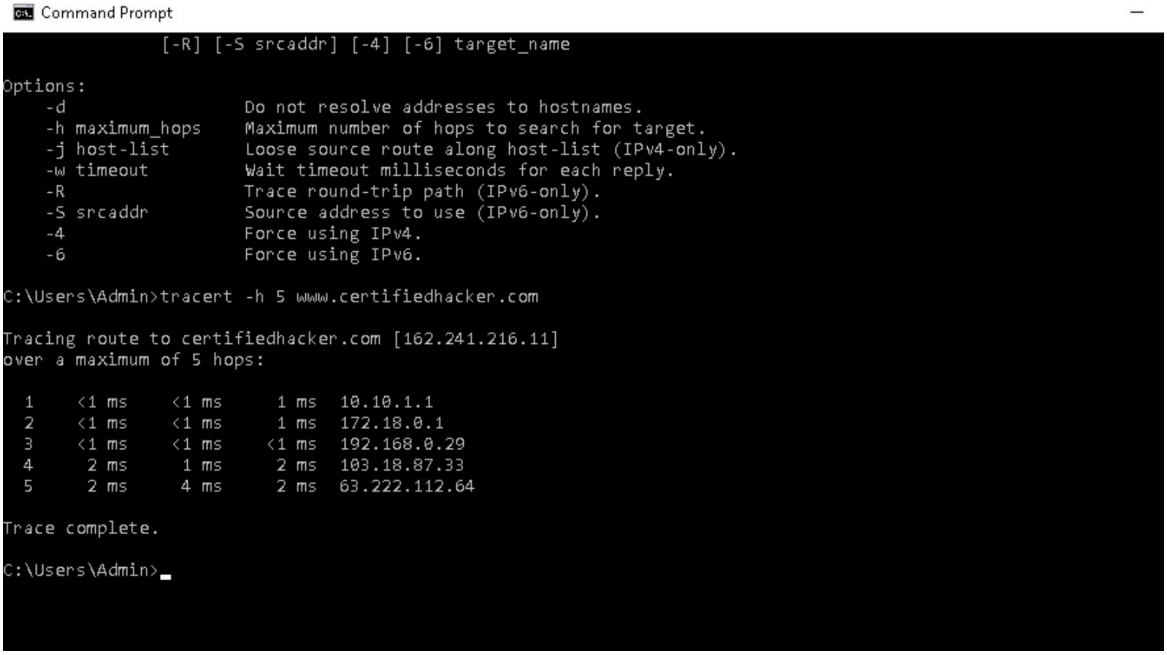
- open the **Command Prompt** window. Type **tracert www.certifiedhacker.com** and press **Enter** to view the hops that the packets made before reaching the destination



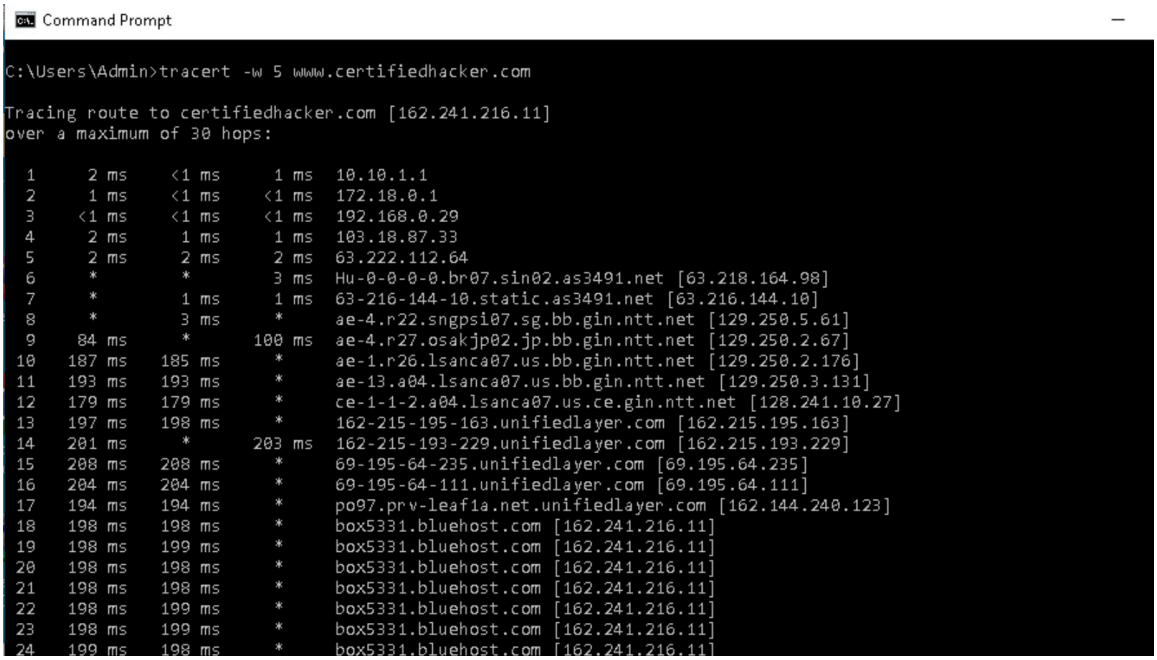
- Type **tracert /?** and press **Enter** to show the different options for the command, as shown in the screenshot.



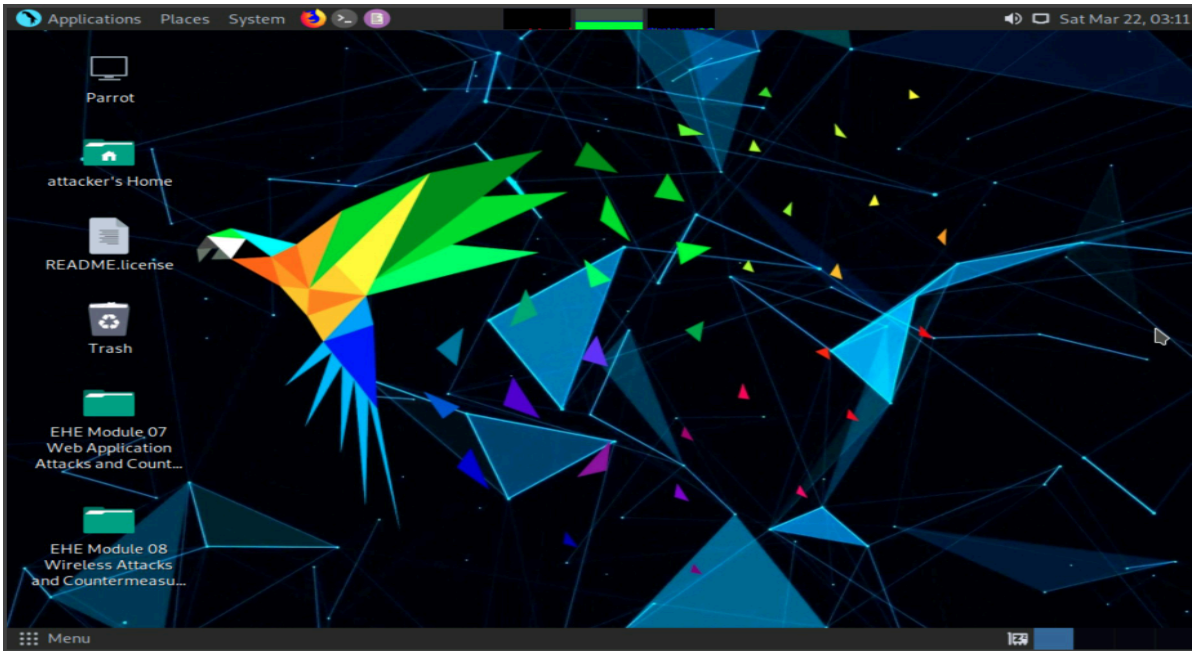
- Type **tracert -h 5 www.certifiedhacker.com** and press **Enter** to perform the trace, but with only 5 maximum hops allowed.



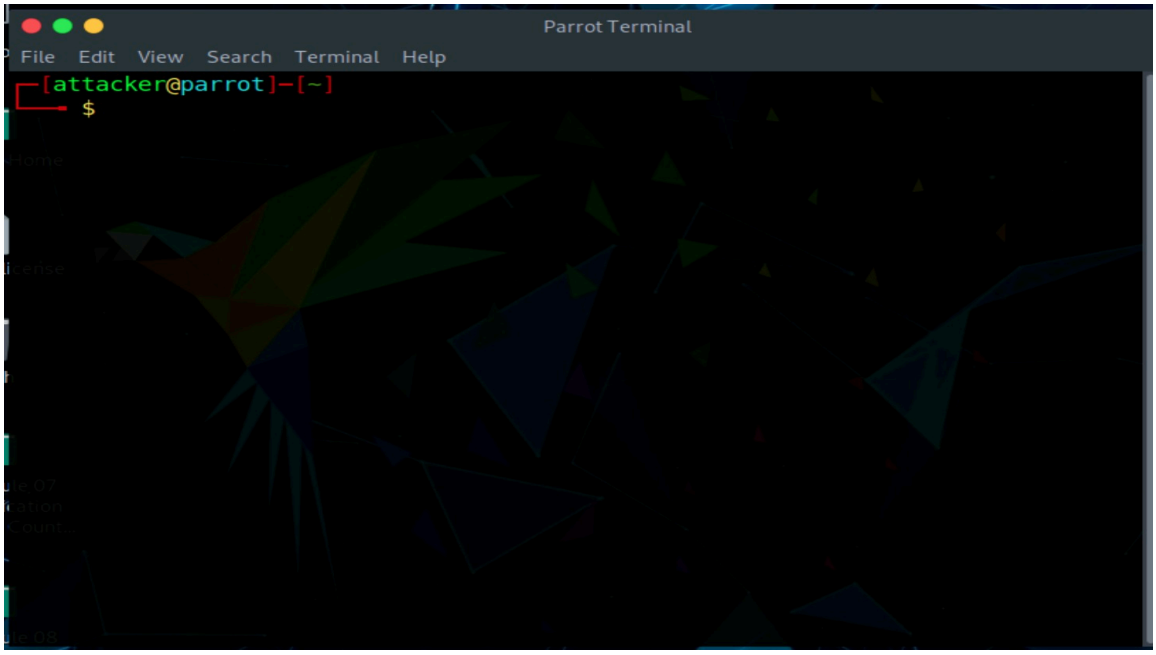
- The results are displayed, as shown in the screenshot.



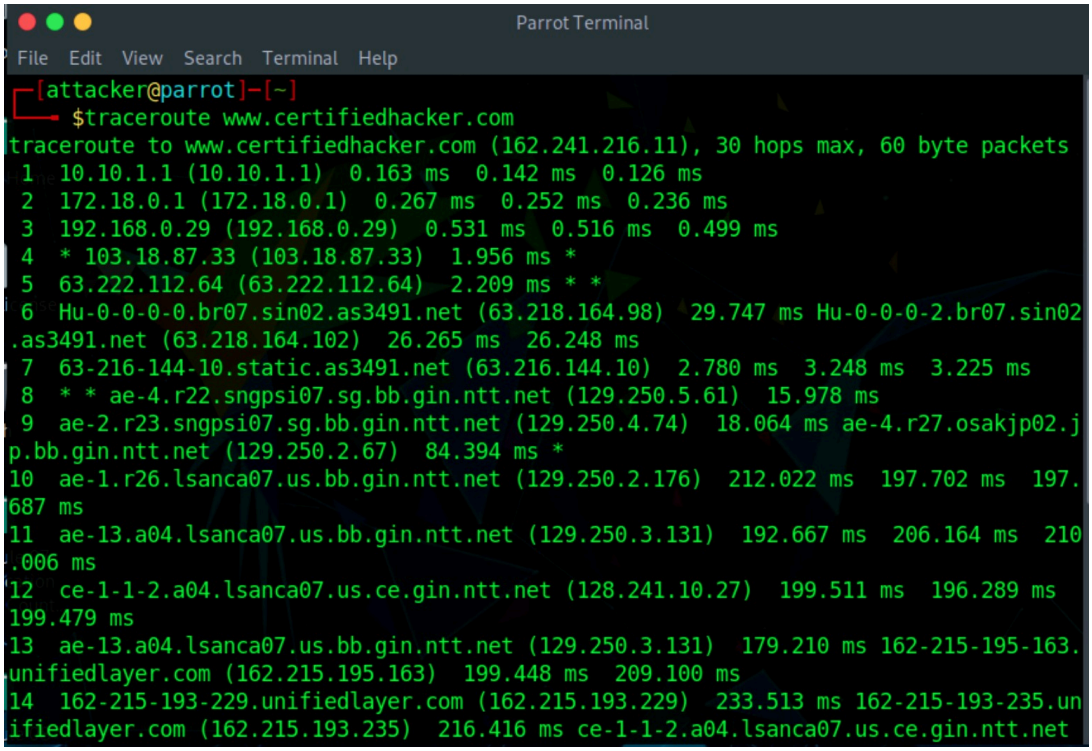
- Now performing same using **Parrot Security 4.10**



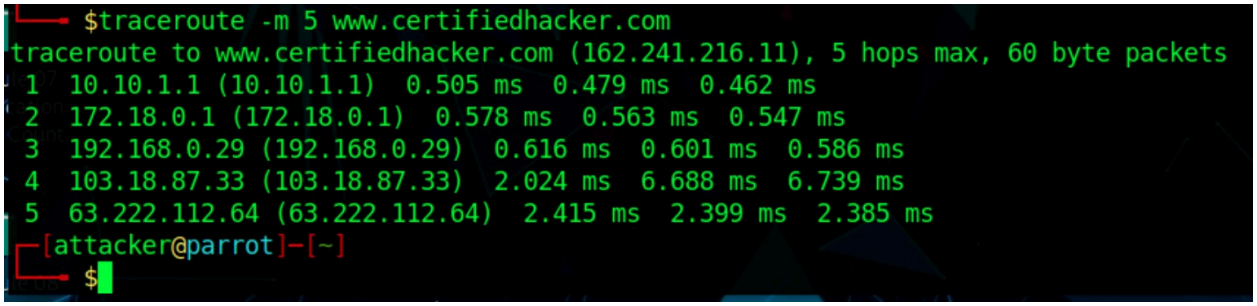
- Open **MATE Terminal** icon at the top-left corner of the **Desktop** window to open a **Terminal** window.



- in the terminal window, type **traceroute** www.certifiedhacker.com **and enter**



- Now, type **traceroute -m 5 www.certifiedhacker.com** and press **Enter** to set the max number of hops as **5** for the packet to reach the destination.



- This concludes the demonstration of performing network tracerouting using the Windows and Linux machines.

Question 2.2.1.1

Perform network tracerouting using traceroute command in Linux machine for www.certifiedhacker.com domain. Enter the IP address of the target domain.

162.241.216.11

Score

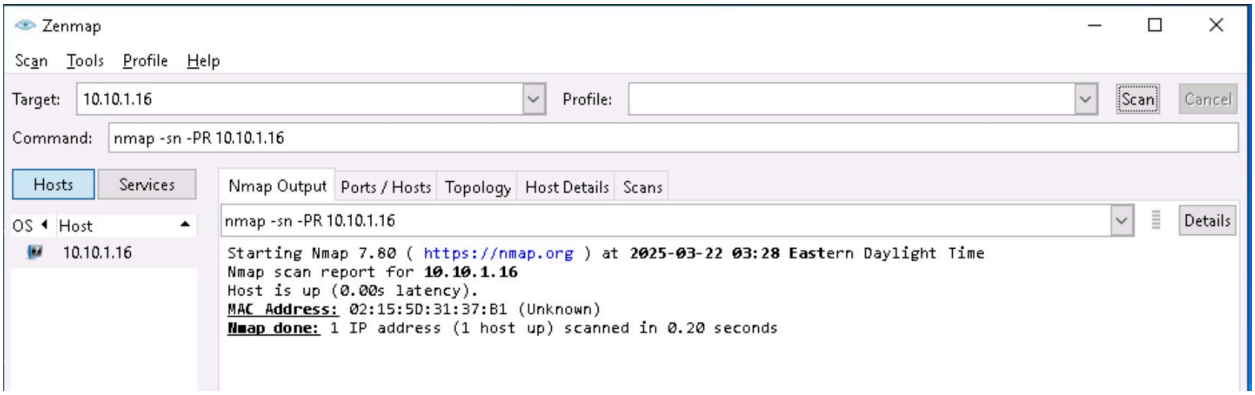
Correct

○ Perform host discovery using Nmap

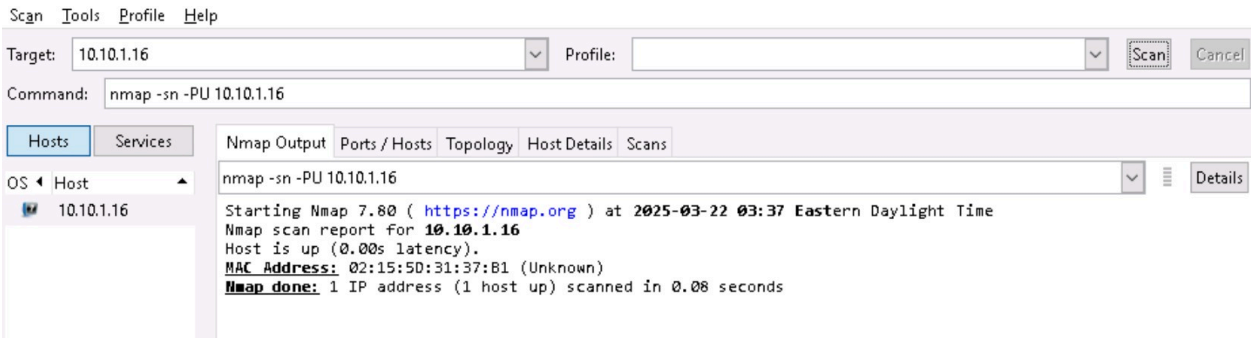
Nmap is a tool for **network discovery, administration, and security auditing**. It helps with **network inventory, service monitoring, and uptime tracking**. Nmap can scan **live hosts** in a target network using techniques like **ARP ping scan, UDP ping scan, and ICMP ECHO ping scan**.

- Click on window 10 to switch to window 10.
- Navigate to the Desktop and double-click **Nmap - Zenmap GUI**

- In the **Command** field, type **nmap -sn -PR [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-sn**: Disables port scanning.
- **-PR**: Performs an **ARP ping scan**.
- The scan results will confirm if the **target Windows Server 2016 (10.10.1.16) host is active**. ● An **ARP request** is sent, and an **ARP response** indicates the host is **up**.

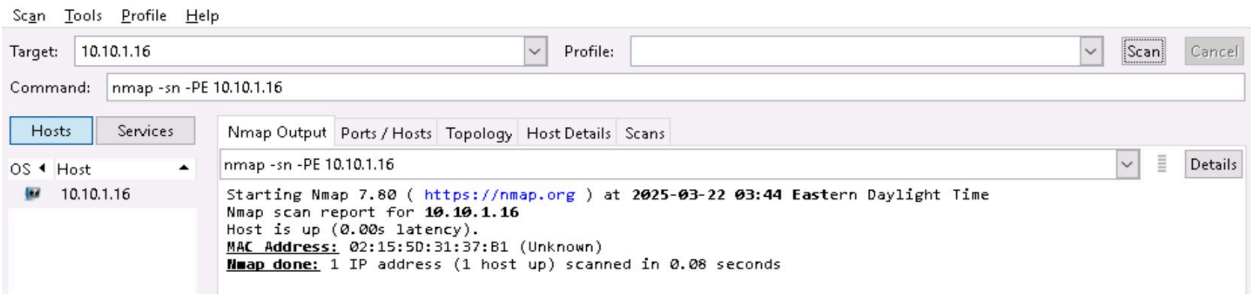


- In the **Command** field, type **nmap -sn -PU [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PU**: Performs a **UDP ping scan**.
- The scan sends **UDP packets** to the target. A **UDP response** confirms the host is **active**.
- If the host is **offline or unreachable**, error messages like **"host/network unreachable"** or **"TTL exceeded"** may appear.

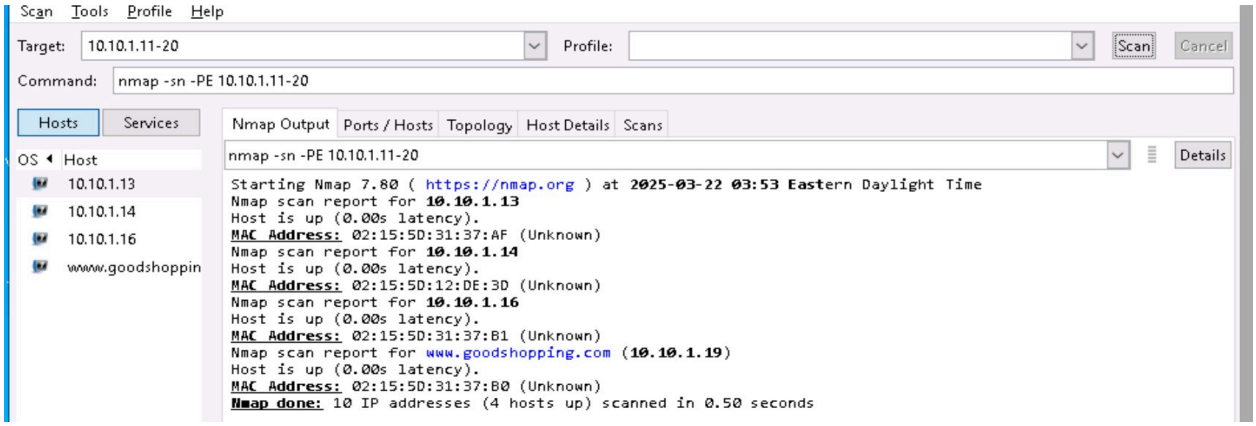


- To perform an **ICMP ECHO ping scan**, type **nmap -sn -PE [Target IP Address]** (e.g., **10.10.1.16**) in the **Command** field and click **Scan**.

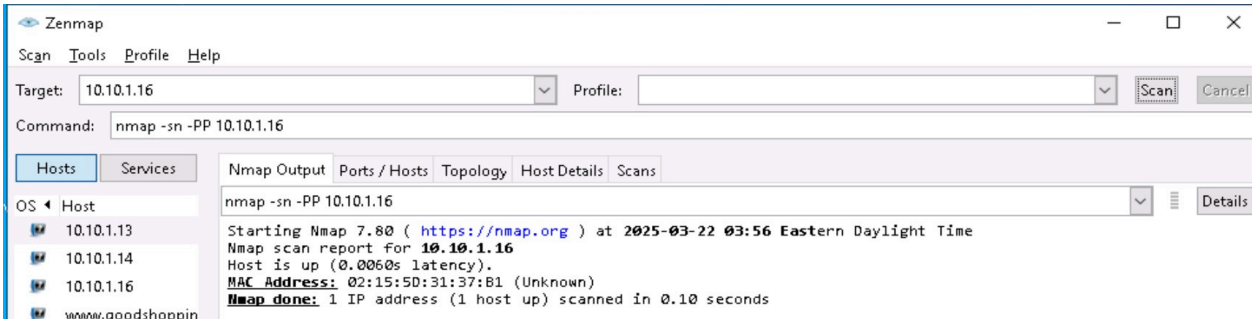
○ The results will indicate if the **target host is up**.
○ **-PE**: Executes an **ICMP ECHO ping scan**.



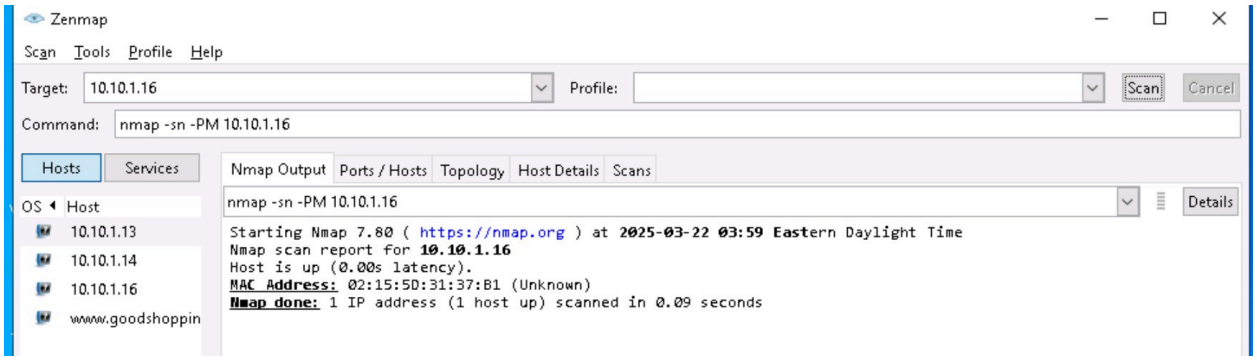
- In the **Command** field, type **nmap -sn -PE [Target Range of IP Addresses]** (e.g., **10.10.1.11-20**) and click **Scan**.
- **-PE**: Performs an **ICMP ECHO ping sweep**.
- This scan sends **ICMP ECHO requests** to multiple hosts to identify **live hosts**. If a host is **active**, it replies with an **ICMP ECHO response**.



- In the **Command** field, type **nmap -sn -PP [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
  - **-PP**: Performs an **ICMP timestamp ping scan**.
- This scan sends **ICMP timestamp requests** to the target. If the target is **active**, it responds with a **timestamp reply**, providing information about the system's current time.



- In the **Command** field, type **nmap -sn -PM [Target IP Address]** (e.g., **10.10.1.16**) and click **Scan**.
- **-PM**: Performs an **ICMP address mask ping scan**.
- This scan sends an **ICMP address mask query** to the target to retrieve **subnet mask information**. It helps identify **active hosts**, especially when **ICMP Echo requests** are blocked by the administrator.



- Other techniques are:
  - **PM**: Performs the **ICMP address mask ping scan**.
  - **PP**: Performs the **ICMP timestamp ping scan**.
  - **TCP SYN Ping Scan**: Sends empty TCP SYN packets to the target host; an **ACK response** means that the host is active.
    nmap -sn -PS [target IP address]
  - **TCP ACK Ping Scan**: Sends empty TCP ACK packets to the target host; an **RST response** means that the host is active.
    nmap -sn -PA [target IP address]
  - **IP Protocol Ping Scan**: Sends probe packets of different IP protocols to the target host; **any response** indicates that a host is active. **nmap -sn -PO [target IP address]**

Question 2.2.2.1

Perform host discovery using Nmap and find the IP address of the machine hosting www.goodshopping.com.

10.10.1.19

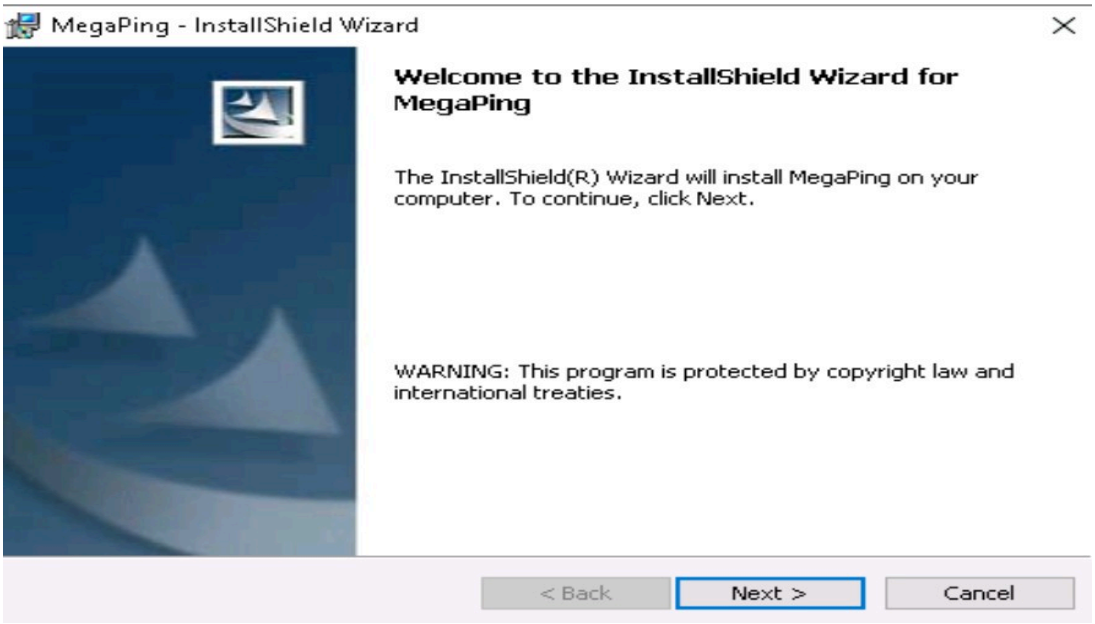
Score

Correct

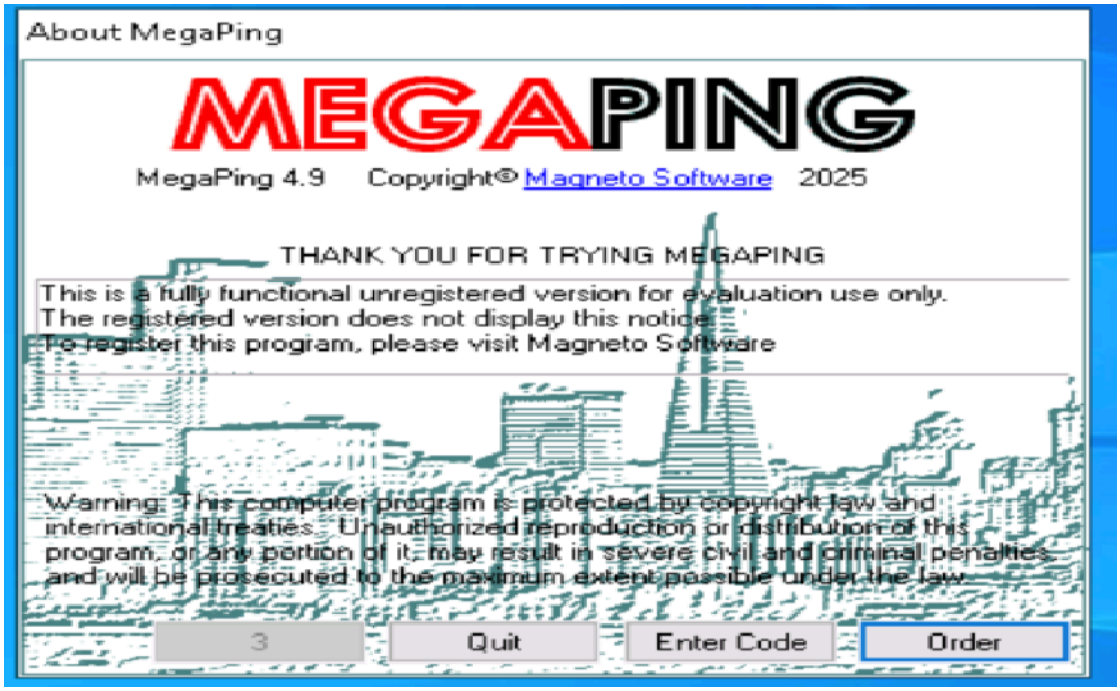
○ Perform port and service discovery using MegaPing

MegaPing is a powerful toolkit designed for IT professionals, system administrators, and security experts. It helps detect live hosts, scan open ports, and gather detailed system and network information. MegaPing can scan an entire network and provide details on shared resources, active services, registry entries, users, groups, trusted domains, and printers. Additionally, it includes network troubleshooting tools such as DNS lookup, IP and NetBIOS scanning, ping, port scanning, traceroute, and Whois.

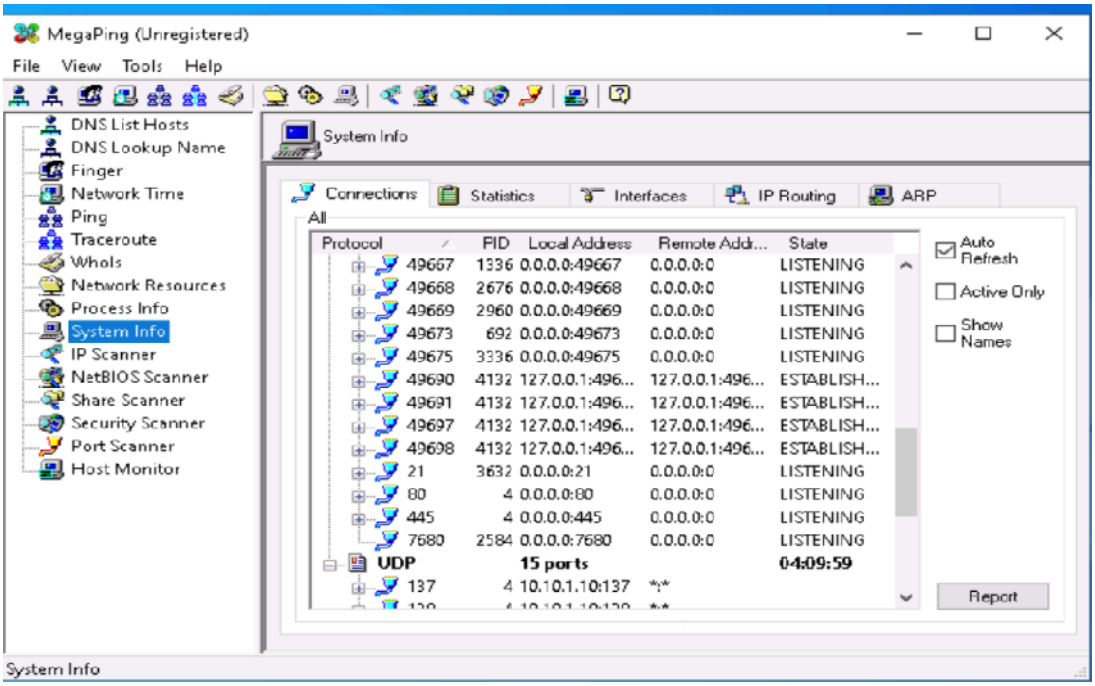
- **InstallShield Wizard** window appears; click **Next** and follow the wizard-driven installation steps to install **MegaPing**.
- After the completion of the installation, click on the **Launch the program**



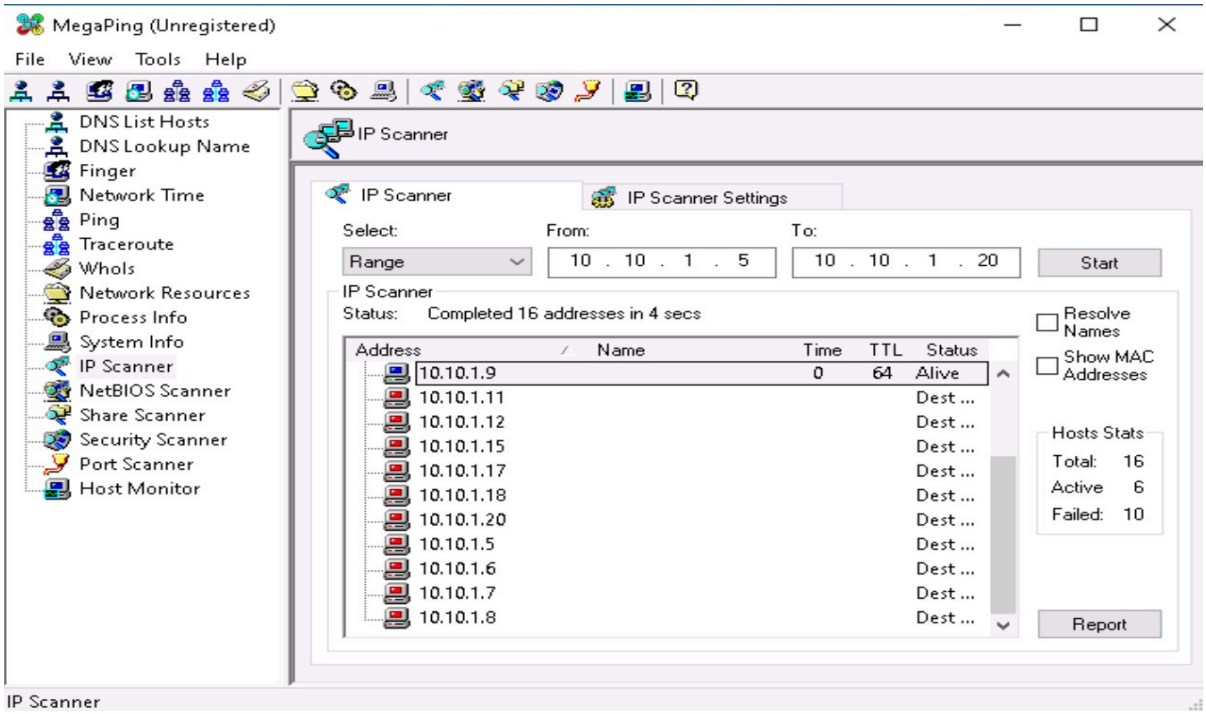
- The **About MegaPing** window appears; click the **I Agree** button.



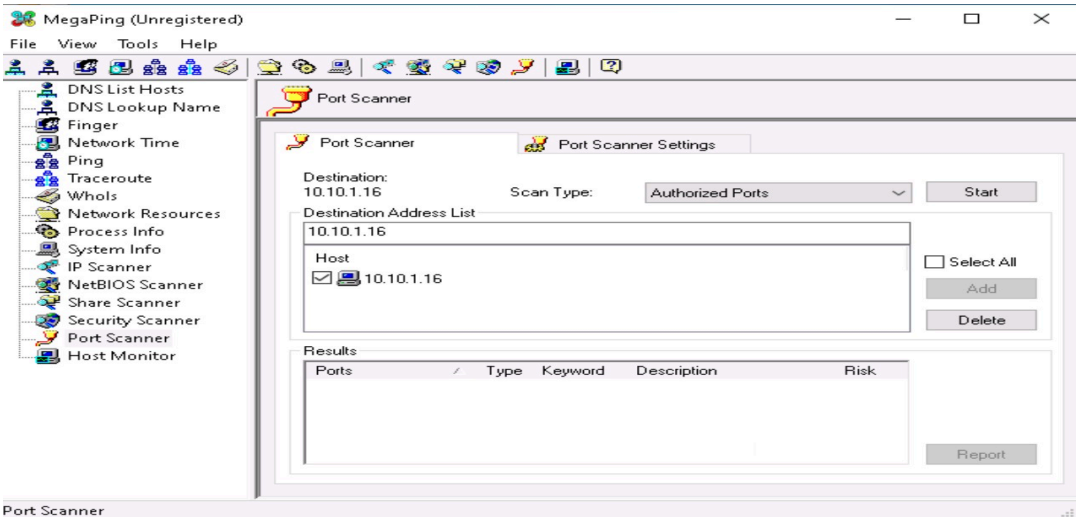
- The **MegaPing (Unregistered)** GUI appears displaying the **System Info**



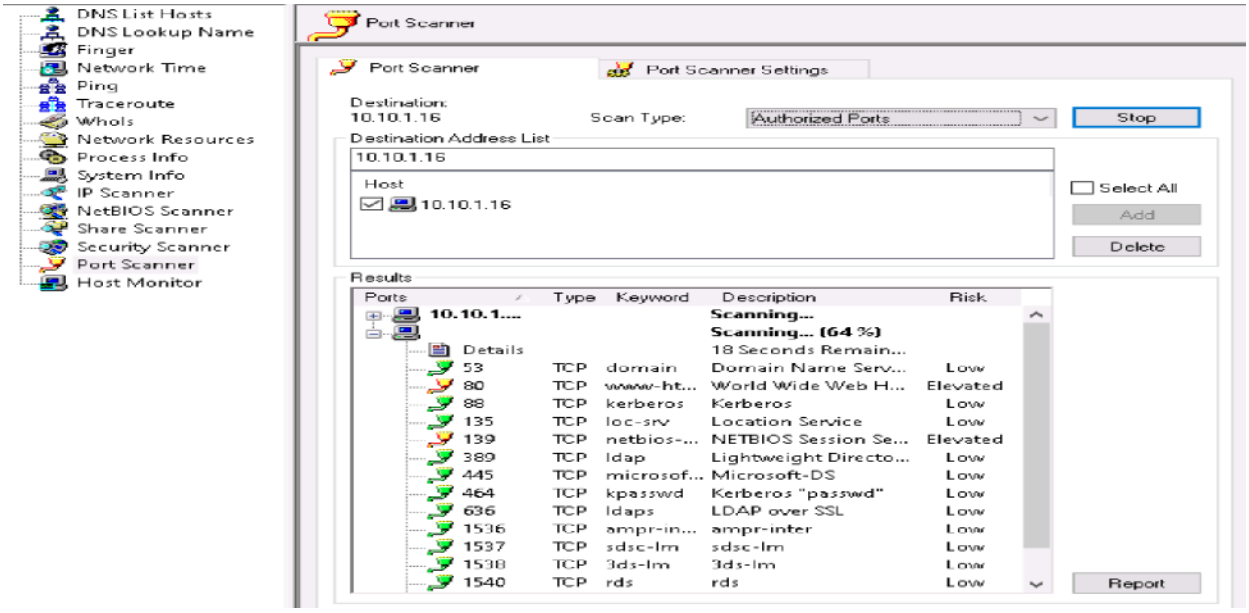
- Select the **IP Scanner** option from the left pane. In the **IP Scanner** tab on the right-hand pane, enter the IP range in the **From** and **To** fields. In this lab, the IP range is **10.10.1.5 to 10.10.1.20**. Then, click **Start** to begin the scanning process.
- MegaPing displays all IP addresses within the specified target range, along with their **TTL value**, **Status** (dead or alive), and statistics of the **dead and alive hosts**, as shown in the screenshot.



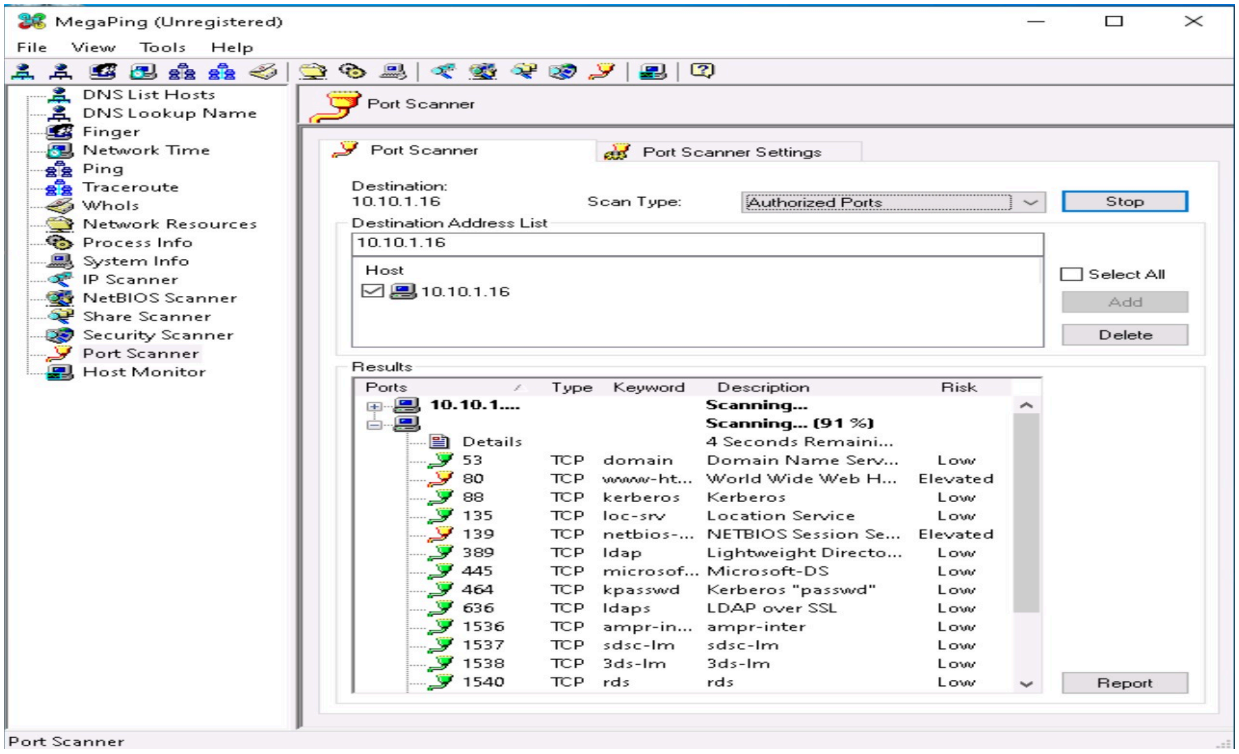
- Select the **Port Scanner** option from the left-hand pane. In the **Port Scanner** tab on the right, enter the **IP address** of the **Windows Server 2016 (10.10.1.16)** machine into the **Destination Address List** field and click **Add.**



- Select the **10.10.1.16** checkbox and click the **Start** button to start listening to the traffic on 10.10.1.16.



- MegaPing displays the **ports** associated with **Windows Server 2016 (10.10.1.16)**, providing details such as the **port number and type, the service running on the port, a description of the service, and the associated risk**, as shown in the screenshot.



Question 2.2.3.1

Perform port and service discovery using MegaPing available at Z:\EHE Module 02 Ethical Hacking Fundamentals\Scanning Tools\MegaPing and name the service running on port 389 on Windows Server 2016 machine.

Ldap

Score

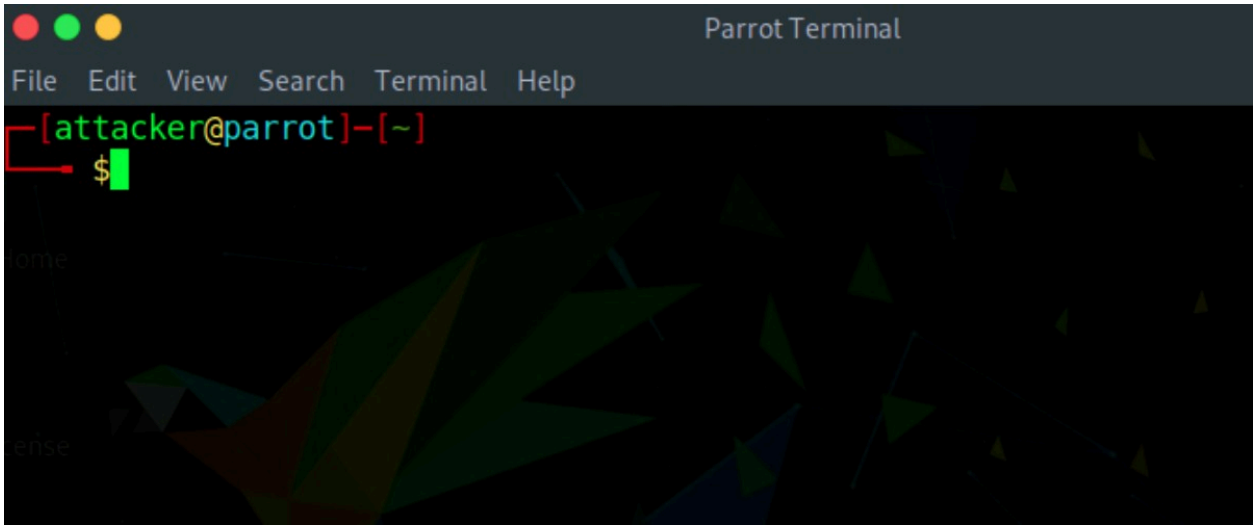
✓ Correct

○ Perform OS discovery using Unicornscan

Unicornscan is a Linux-based command-line tool for network reconnaissance and information gathering. It is an asynchronous TCP and UDP port scanner and banner grabber used to discover open ports, services, TTL values, and more on a target machine. By analyzing TTL values in the scan results, Unicornscan can help identify the operating system of the target machine.

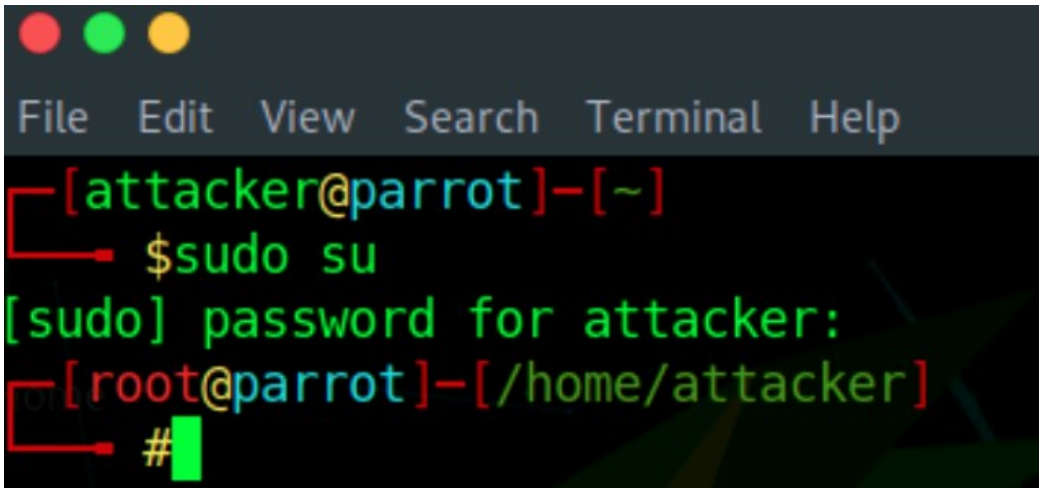
In this task, Unicornscan will be used to perform OS discovery on the target system.

- switch to the **Parrot Security** machine.
- Click the **MATE Terminal** icon at the top of the **Desktop** window to open a Terminal window. ● **Open the Parrot Terminal**

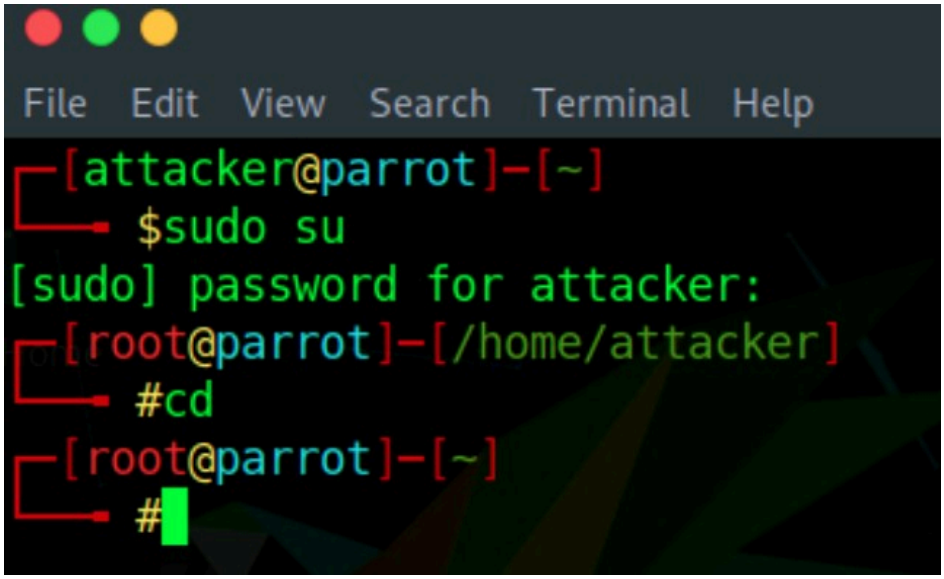


- **Switch to Root User**:
  - Type: sudo su and press enter
- **Enter Password**:
  - In [sudo] password for attacker: field, type: toor
  - Press **Enter**

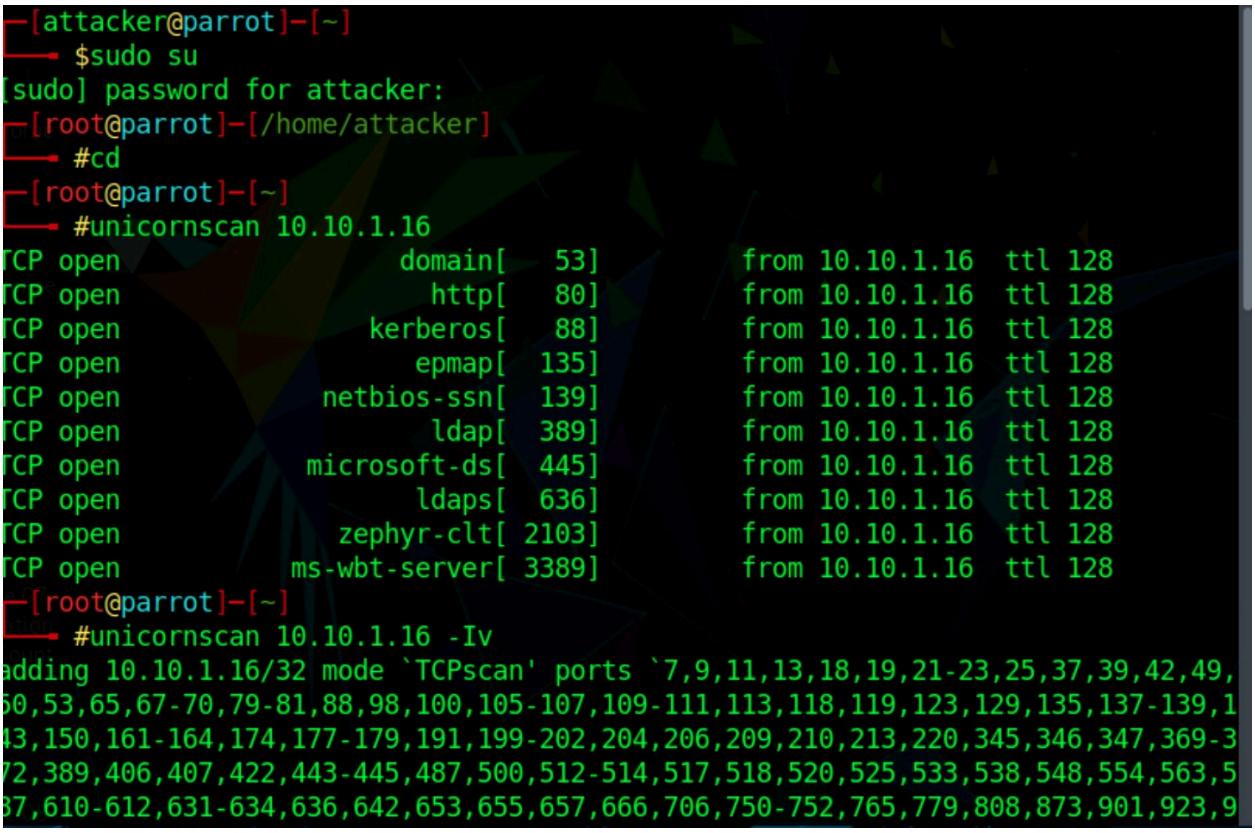
    (Note: The password will not be visible while typing.)



- **Navigate to the Root Directory**:
  - Type: cd and Press **Enter**



- Now, you are in the root environment and ready to execute **Unicornscan** commands.

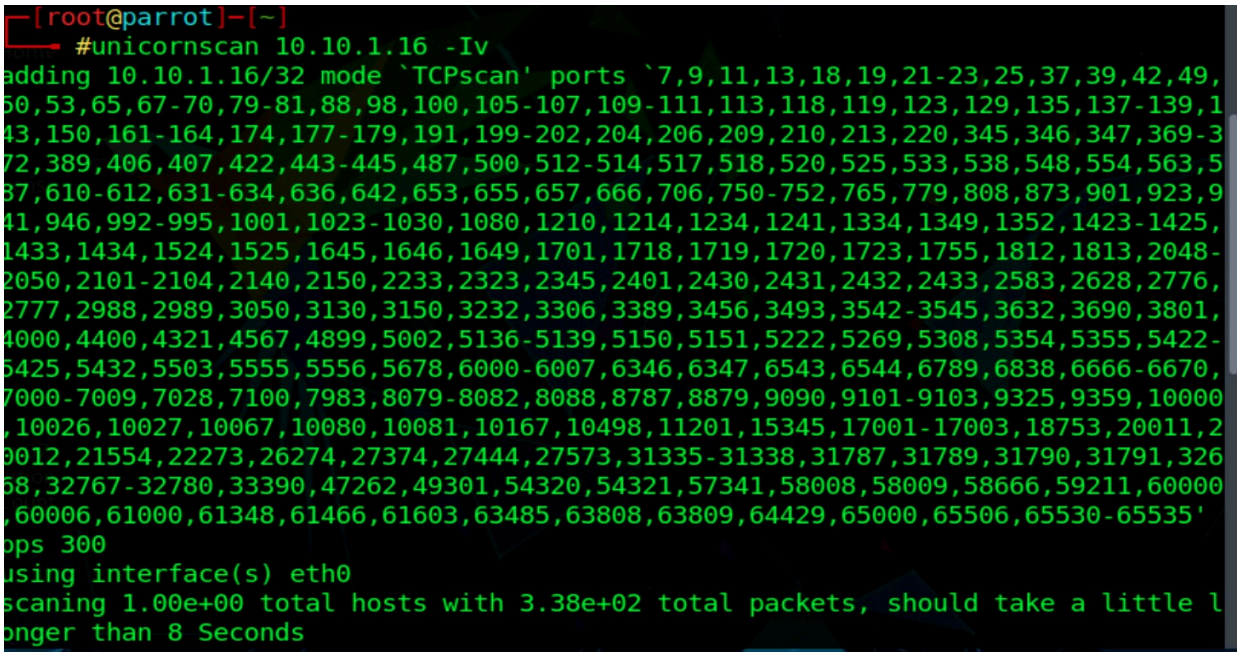


- The command **unicornscan 10.10.1.16 -Iv** is used to perform a detailed scan on the target machine, which in this case is a **Windows Server 2016** with the IP address **10.10.1.16**.
- **unicornscan** → Runs Unicornscan, a network reconnaissance tool.
- **10.10.1.16** → Specifies the target IP address.
- **-I** → Enables **immediate mode** for faster scanning.
- **v** → Enables **verbose mode** to display detailed scan results.

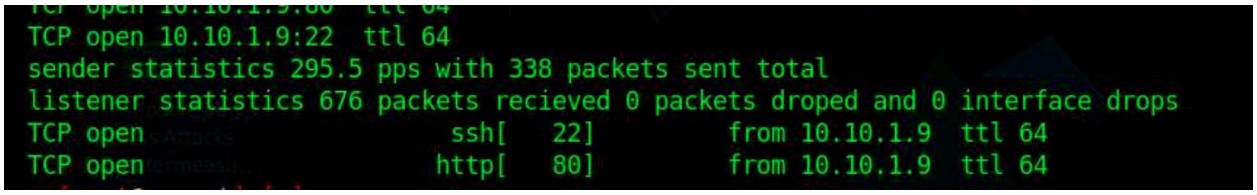
The scan detects **open TCP ports**, **running services**, and the **TTL value** of **128**, indicating that the

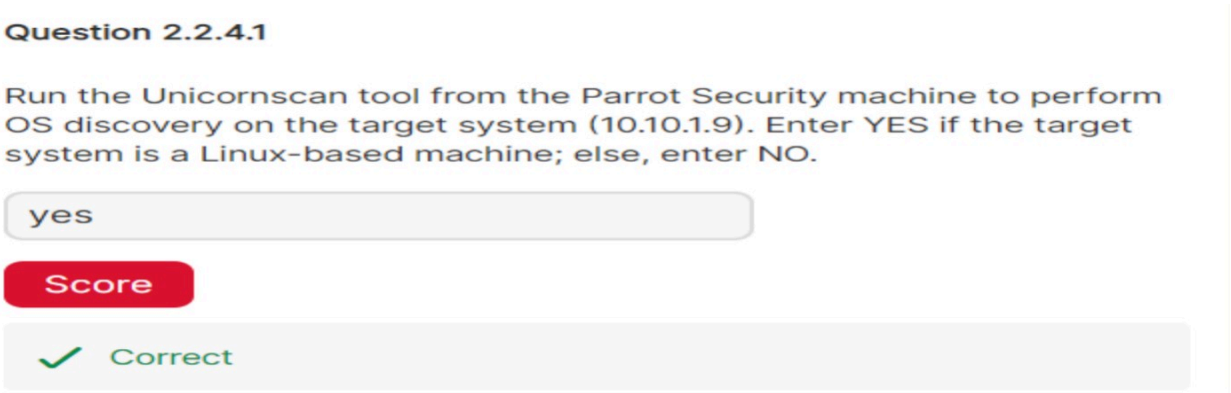
target OS is likely **Microsoft Windows (Windows 7/8/8.1/10 or Windows Server 2008/12/16)**.

- The command **unicornscan 10.10.1.9 -Iv** is used to perform a detailed scan on the target machine, which in this case is **Ubuntu (10.10.1.9)**.



The scan detects **open TCP ports**, **running services**, and a **TTL value of 64**, indicating that the target OS is likely **Linux-based (Google Linux, Ubuntu, Parrot, or Kali)**.





- Perform enumeration on a system or network to extract usernames, machine names, network resources, shares, etc.

Enumeration is the process of actively gathering detailed information about a target system by establishing a connection and performing queries. It helps in identifying usernames, user groups, shared folders, active services, open ports, OS type, machine name, and network configuration. Enumeration techniques are conducted in intranet environments to identify vulnerabilities for security analysis or exploitation.

■ Perform NetBIOS enumeration using Windows Command-Line utilities

■ First switch to the Windows Server 2019 (10.10.1.19) machine and activate it using **Ctrl+Alt+Delete**. Log in with the **Administration** profile by pasting **Pa$$w0rd** in the password field. Alternatively, use the **Type Password** option under the **Commands** menu. When the **Networks** screen appears, click **Yes** to allow network discovery.

■ Run the command:

- **nbtstat -a 10.10.1.10**
- This displays the NetBIOS name table of the remote **Windows 10** machine, revealing active NetBIOS names and their associated types.

```
Microsoft Windows [Version 10.0.17763.1158]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nbtstat -a 10.10.1.10

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    WINDOWS10      <00>  UNIQUE      Registered
    WORKGROUP      <00>  GROUP       Registered
    WINDOWS10      <20>  UNIQUE      Registered
    WORKGROUP      <1E>  GROUP       Registered
    WORKGROUP      <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-15-5D-01-80-01
```

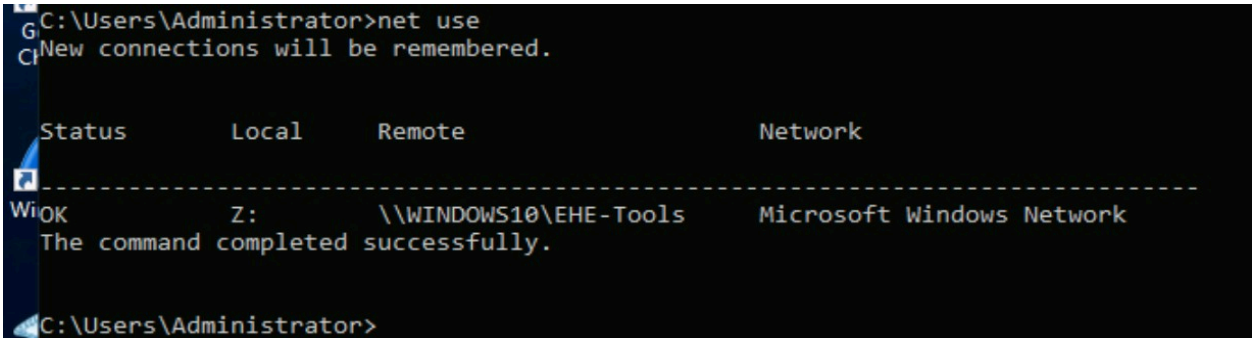
■ NOW Run the command:

- **nbtstat -c**
- This lists the NetBIOS name cache, showing stored NetBIOS names and their resolved IP addresses without requiring authentication.

```
C:\Users\Administrator>nbtstat -c

Ethernet:
Node IpAddress: [10.10.1.19] Scope Id: []

                NetBIOS Remote Cache Name Table

       Name               Type       Host Address    Life [sec]
    ------------------------------------------------------------
    WINDOWS10      <20>  UNIQUE          10.10.1.10          351

C:\Users\Administrator>
```

■ Run the command:

- **net use**
- This displays active network connections, including shared folders, drives, and connection status.



9. This concludes the demonstration of performing NetBIOS enumeration using Windows command-line utilities such as Nbtstat and Net use.

10. Close all open windows and document all the acquired information.

Question 2.3.1.1

Name the shared folder/drive available for the Windows Server 2019 machine.

\\WINDOWS10\EHE-Tools

Score

Correct

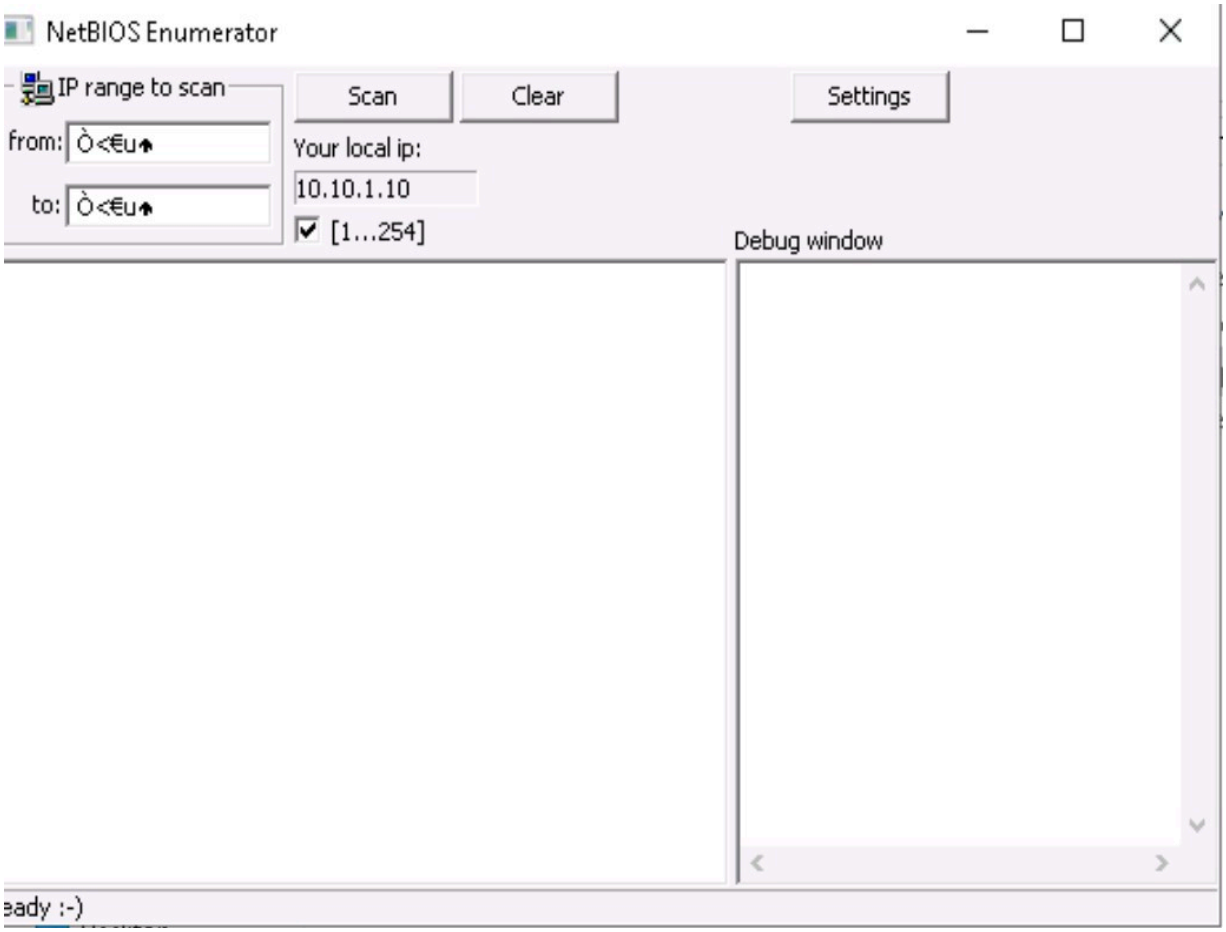
Perform NetBIOS enumeration using NetBIOS Enumerator

NetBIOS Enumerator is a tool for gathering network details like NetBIOS names, usernames, domain names, and MAC addresses using SMB.

Here, a Windows 10 machine is used to perform NetBIOS enumeration on Windows Server 2016 and Windows Server 2019 machines.

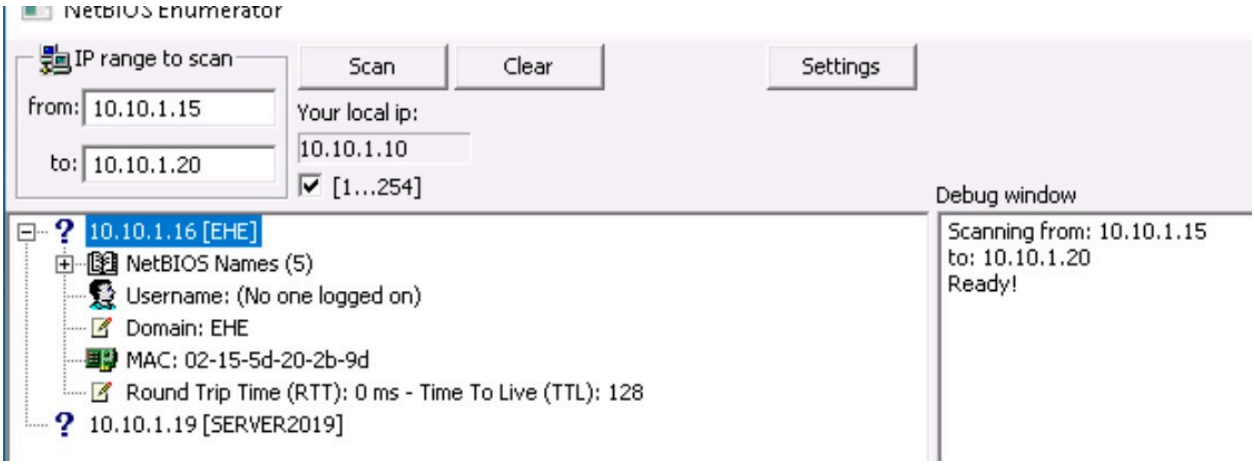
- Switch to the Windows 10 machine.
- Navigate to **D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator** and double-click **NetBIOS Enumerator.exe**.
- If a security warning appears, click **Run**. The NetBIOS Enumerator main window will open.

- The **NetBIOS Enumerator** main window appears, as shown in the screenshot.



- Under **IP range to scan** put IP range **10.10.1.15-10.10.1.20** and click scan.
- NetBIOS Enumerator scans the specified IP address range. Once completed, the scan results appear in the left pane.
- The **Debug window** in the right pane shows the scanning progress and displays **Ready!** when the scan is finished.

- Click the **expand icon (+)** next to **10.10.1.16** and **10.10.1.19** in the left pane to reveal their details.
  - Next, expand **NetBIOS Names** to view the NetBIOS details of the target IP addresses.



8. This concludes the demonstration of performing NetBIOS enumeration using NetBIOS Enumerator. This enumerated NetBIOS information can be used to strategize an attack on the target.

9. Close all open windows and document all the acquired information.

Question 2.3.2.1

Use the NetBIOS Enumerator tool to perform NetBIOS enumeration on the network (10.10.1.15 - 10.10.1.20). NetBIOS Enumerator tool is available at D:\EHE-Tools\EHE Module 02 Ethical Hacking Fundamentals\NetBIOS Enumeration Tools\NetBIOS Enumerator. Enter the domain name associated with the IP address 10.10.1.16.

EHE

Score

Correct

Ethical Hacking Lab Report – 06 (Date: 12-05-2025)

EC-Council Lab Assignment: Module 3

Information Security Threats and Vulnerability Assessment

Scenario

A threat is a possible event that can harm or disrupt an organization's operations. Threats can be physical or digital, and may be accidental, intentional, or due to other causes. Cyber threats often target personal, financial, and login data, and compromised systems may be used for further malicious actions. The severity of a threat depends on its potential damage, detection difficulty, and control level. Threats can compromise the

Confidentiality, Integrity, and Availability (CIA) of data, causing data loss, identity theft, and other cybercrimes.

In this module's labs, you'll explore how attackers create and spread malware, and how to assess vulnerabilities in systems and networks.

Objective

This lab helps you:

- Create and deploy a Trojan to exploit a target system
- Develop a virus to infect a target machine
- Perform vulnerability assessments to find system/network weaknesses

Overview of Threats

Types of Threats:

- Natural Threats: Disasters like floods, fires, earthquakes, and power failures that can damage IT infrastructure.
- Unintentional Threats: Human errors, poor training, or negligence within an organization.
- Intentional Threats:
    - Internal: Insider threats by employees with access to systems
    - External: Attackers exploiting system vulnerabilities from outside

Lab 1: Create a Trojan to Gain Access to the Target System

Scenario

A Trojan disguises itself as a legitimate program but secretly performs harmful actions. Attackers may use it to control systems remotely, steal data, or launch other attacks. Systems using unencrypted credentials are especially vulnerable. Trojans can enter via email, downloads, or instant messaging and may spoof their origin to mislead investigations.

This lab shows how attackers take control of systems using Trojans and establish hidden channels for data transfer.

Objectives

- Create a Trojan Server with Theef RAT
- Control a Victim System using njRAT

Task 1: Create a Trojan Server using Theef RAT Trojan

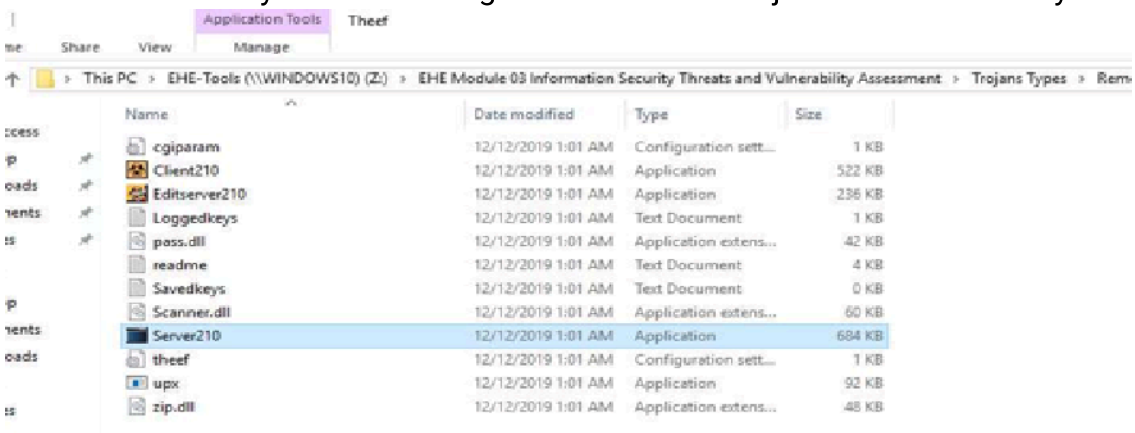
Remote Access Trojans (RATs) let attackers gain full remote control of a system, including screen and webcam access, file management, keylogging, and command execution. These RATs spread via phishing, USB drives, or drive-by downloads.

Theef RAT, written in Delphi, operates over port 9871 and consists of a client (attacker's control panel) and server (malicious file installed on the victim's system). Though interface versions may differ, the creation process remains consistent

In this lab, for demonstration purposes, we are directly executing the file on the victim machine, **Windows Server 2016**. And **Windows 10** machine (as an attacker)

On the Victim's Machine (Windows Server 2016)

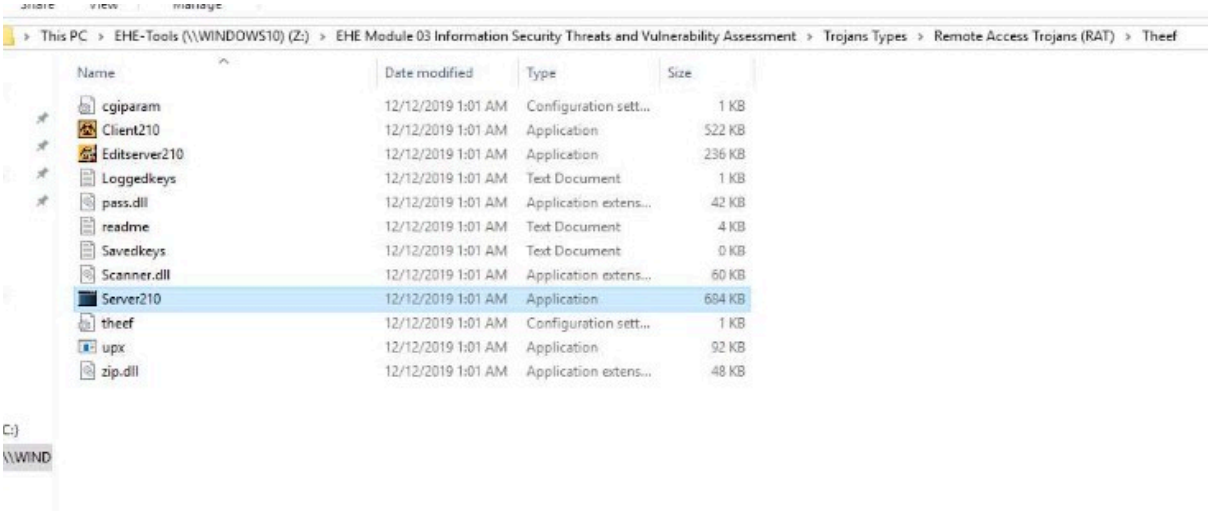
1. Navigate to:
   Z:\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Run Server210.exe by double-clicking it to initiate the Trojan on the victim's system.



On the Attacker's Machine (Windows 10)

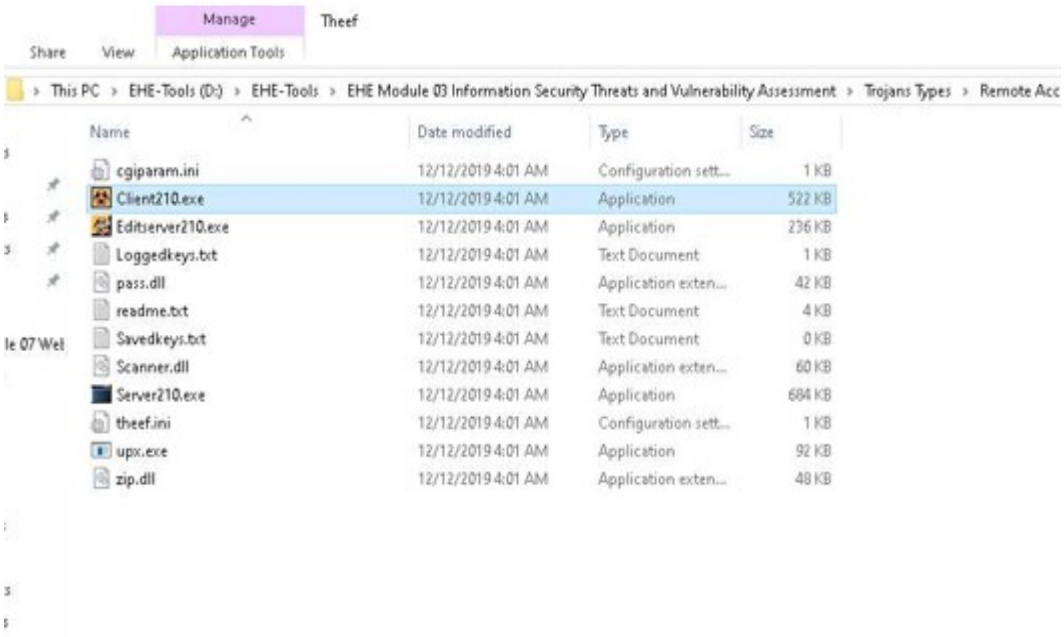
1. Navigate to:
   D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef
2. Launch Client210.exe to open the attack interface.
3. Enter the **IP address** of the victim machine.
4. A remote session is successfully established with the Windows Server 2016

system

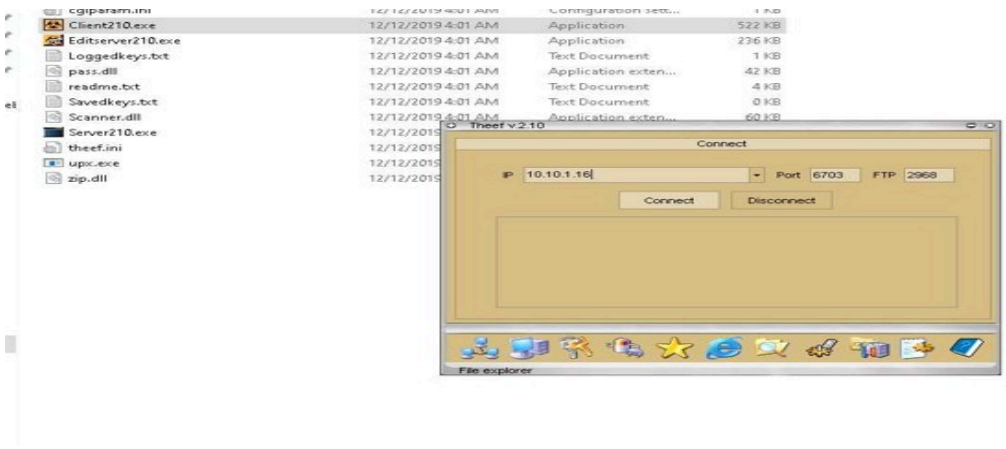


In Attackers machine

Navigate to **D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\Theef** and double-click **Client210.exe** to access the victim machine remotely.



Enter the IP address of the victim's system.



From **Windows 10**, we have successfully established a remote connection with the **Windows Server 2016** machine.

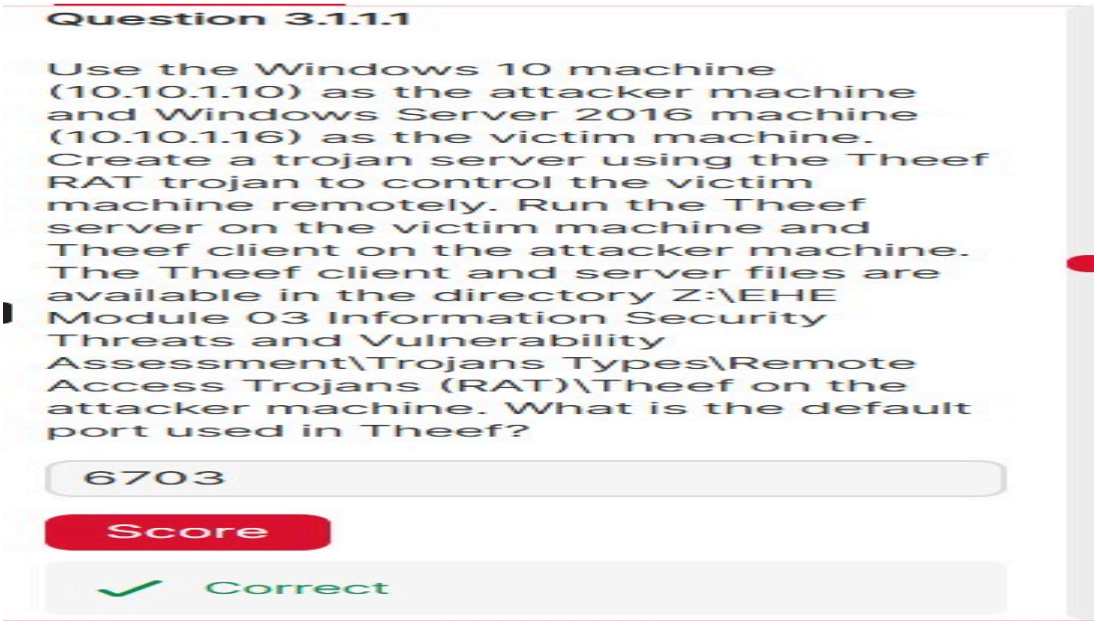
1. In **Computer Information**, we can view **PC Details**, **OS Info**, **Home**, and **Network** by clicking their respective buttons.

Here, for example, selecting **PC Details** reveals computer-related information

Spy icon to perform various operations like capture screens, log keys, view processes, view the task manager, use the webcam, and use the microphone on the target machine

For instance, selecting **Task Manager** views the tasks running on the target machine

Similarly For capturing keylogger event of the victim computer. Attacker's System



Task 2: Gain Control over a Victim Machine using the njRAT RAT Trojan

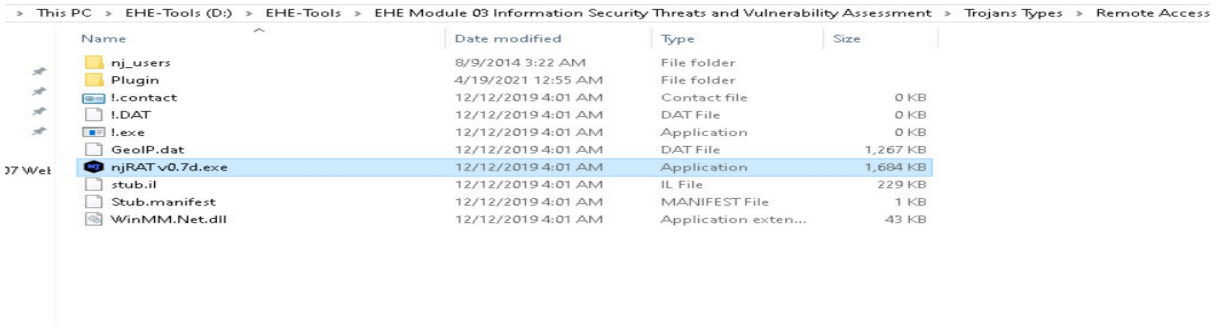
njRAT is a Remote Access Trojan (RAT) with advanced data-stealing features. It can log keystrokes, access the victim's camera, steal credentials stored in browsers, upload and download files, manipulate processes and files, and view the victim's desktop.

This RAT also allows attackers to control Botnets (networks of compromised computers), enabling them to update, uninstall, disconnect, restart, and terminate the

RAT, as well as rename its campaign ID. Additionally, it can be configured to spread through USB drives using the Command and Control server software.

In this lab exercise, we will use **njRAT** to take control of a victim machine. The **attacker machine** will be a Windows 10 machine (IP: 10.10.1.10), and the **victim machine** will be a Windows Server 2016 (IP: 10.10.1.16).

To begin, on the **Windows 10 machine**, navigate to:
D:\EHE-Tools\EHE Module 03 Information Security Threats and Vulnerability Assessment\Trojans Types\Remote Access Trojans (RAT)\njRAT and double-click on njRAT v0.7d.exe.



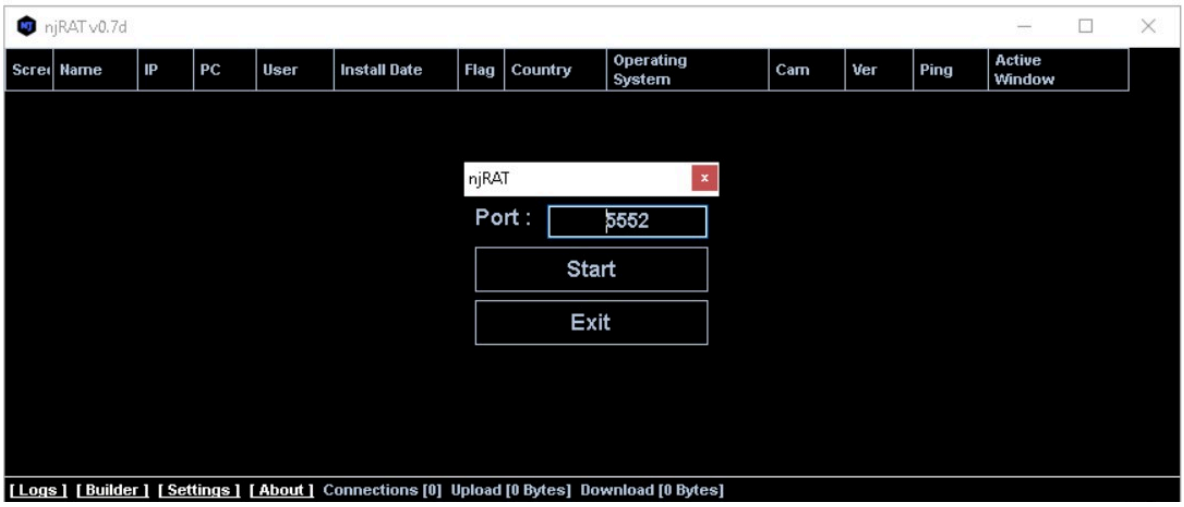
njRAT is a Remote Access Trojan that enables automatic reconnection and provides a wide range of spying and control functionalities.

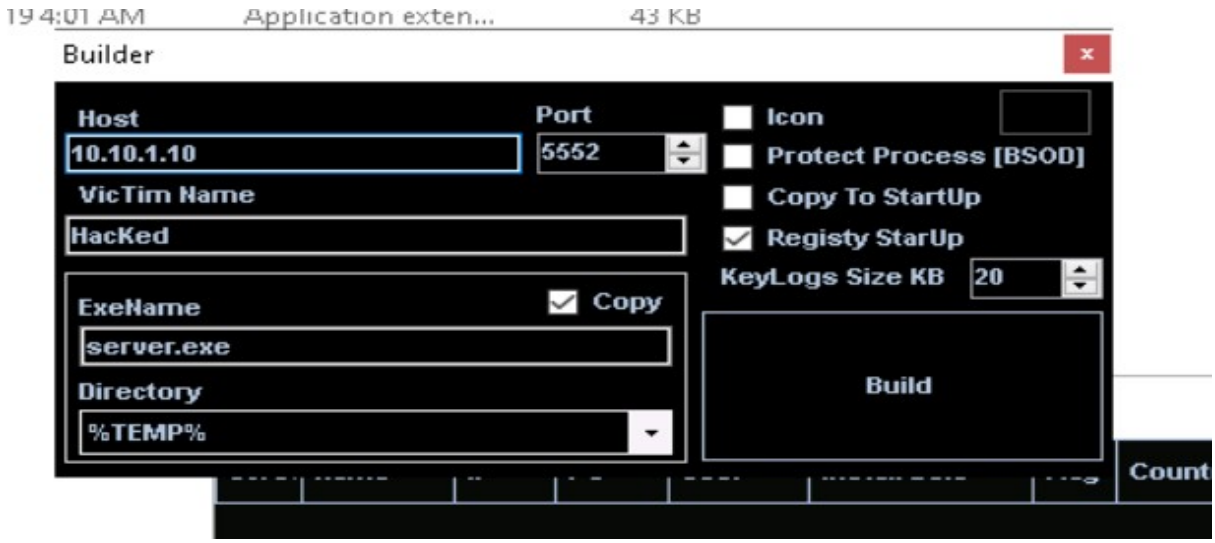
Steps to Configure njRAT:

1. **Launch njRAT**:
   Open the njRAT GUI. A pop-up appears asking for the port number.
2. **Set Port Number**:
   Enter the desired port — **5552** is used in this lab — and click **Start**.
3. **Configure Server Using Builder**:
   - Click the **Builder** button (bottom-left of the njRAT interface).
   - In the **Builder** dialog:
     - **Host**: Enter the IP address of the attacker's machine — 10.10.1.10.

- **Enable**: Check the **Registry Startup** option.
- Leave other settings as default.
- Click **Build**.

4. **Save the Server File**:
    - When prompted with the **Save As** dialog:
        - Save the file to the **Desktop**.
        - Name it Test.exe.
        - Click **Save**.
5. **Build Confirmation**:
   After successful creation, a "DONE!" message appears. Click **OK** to finish

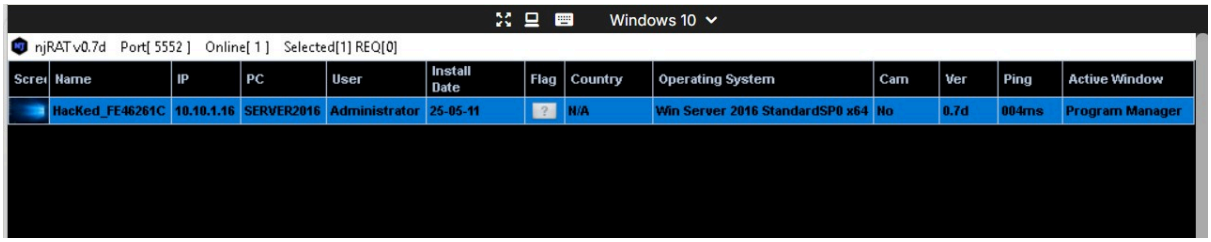




Switch to Windows server 2016 and Navigate to the shared network location (EHE-Tools), and then Copy and Paste the executable file (Test.exe) onto the Desktop of Windows Server 2016.

Double-click the server (Test.exe) to run this malicious executable

Click Windows 10 to switch back to the Windows 10 machine. As soon as the victim (here, you) double-clicks the server, the executable starts running and the njRAT client (njRAT GUI) running in Windows 10 establishes a persistent connection with the victim machine, as shown in the screenshot



Once a connection is established, **njRAT GUI** displays key details about the compromised system, including:

- **IP Address**
- **Username**
- **Operating System**

Steps to Control the Victim System:

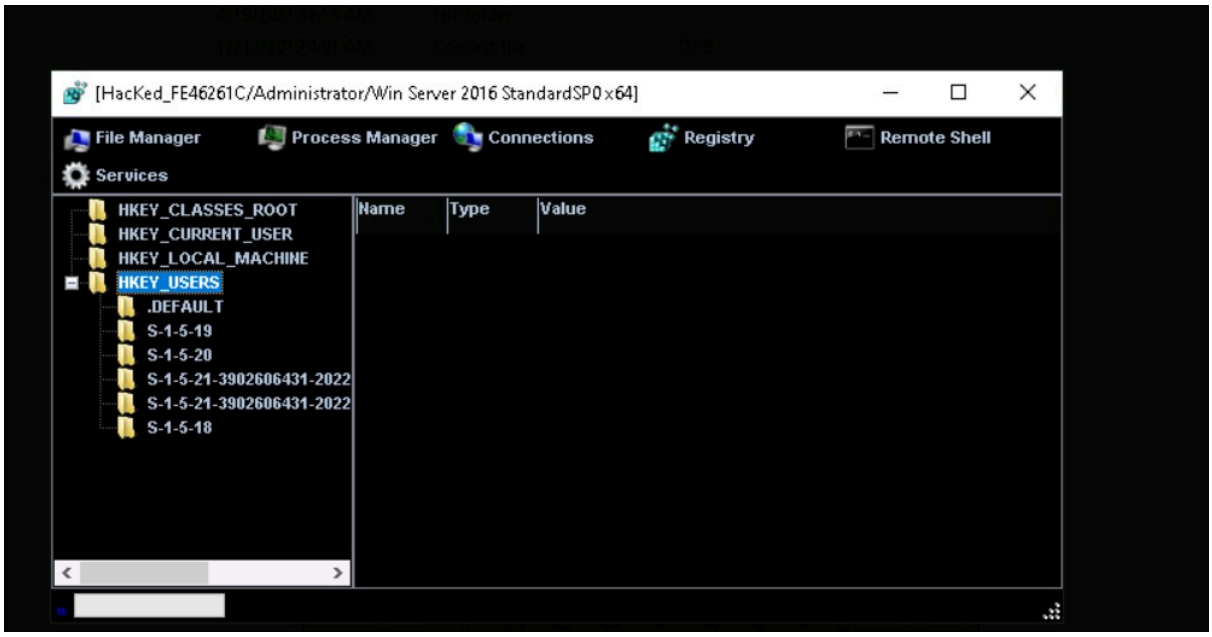
1. **Access Control Options**:
    - Right-click on the victim machine listed in the njRAT interface.
    - Select **Manager** from the context menu.
2. **File Manager Tab**:
    - Opens by default in the Manager window.
    - Double-click any folder on the left panel (e.g., ProgramData) to browse its contents in the right panel.
    - Right-click on any file or folder to see options like Open, Delete, Rename, or Execute.
3. **Process Manager Tab**:
    - Click the **Process Manager** tab to view all running processes.
    - Right-click on any process to:
        - **Kill** (terminate),
        - **Delete**, or
        - **Restart** it

.

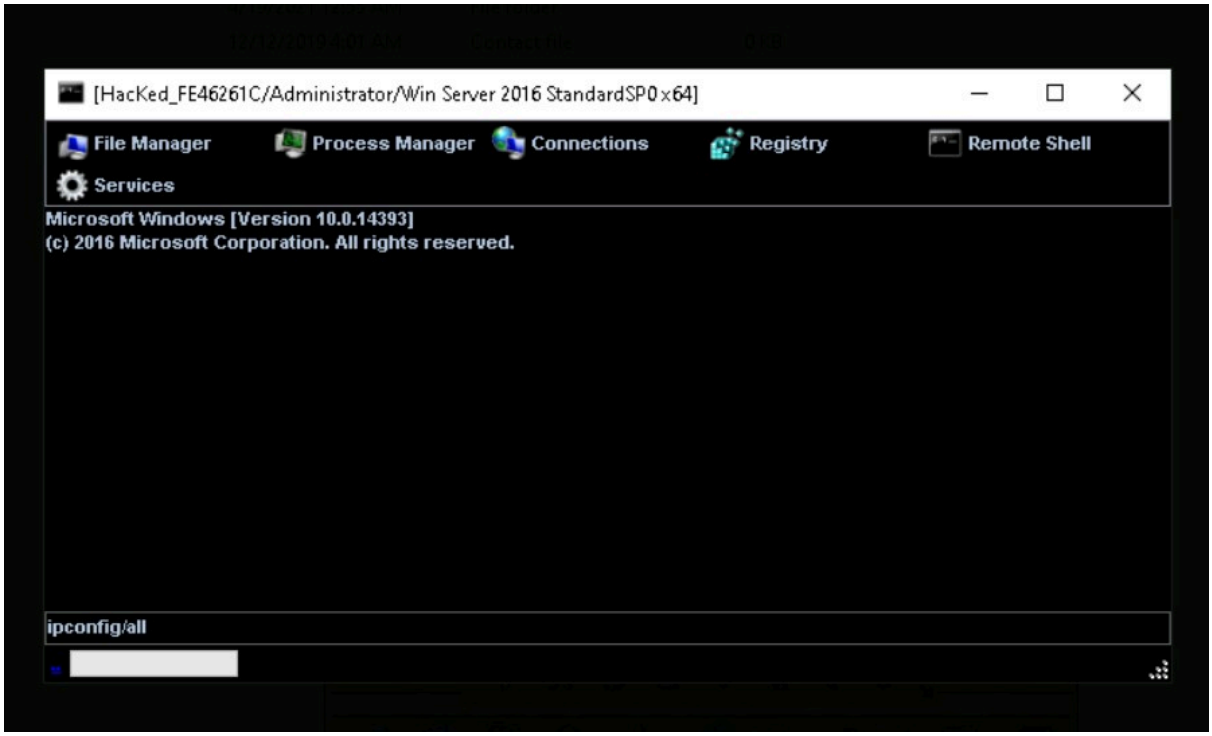
mqsvc.exe	2948	system32	NETWORK SERVICE	
msdtc.exe	3004	System32	NETWORK SERVICE	
nfsclnt.exe	2268	system32	NETWORK SERVICE	
RuntimeBroker.exe	908	System32	Administrator	-Embedding
SearchUI.exe	4476	Microsoft.Windows.Cortana_cw5n1h2txyewy	Administrator	-ServerName:CortanaUI.AppXa50dqqa5gqv4a428c9y1jjw7m3btvepj.mca
server.exe	5888	Temp	Administrator	
services.exe	596		SYSTEM	
ShellExperienceHost.exe	4392	ShellExperienceHost_cw5n1h2txyewy	Administrator	-ServerName:App.AppXtk181tbxbce2qsex02s8tw7hfxa9xb3t.mca
sihost.exe	2192	system32	Administrator	
smss.exe	288		SYSTEM	
SMSvcHost.exe	2932	v4.0.30319	LOCAL SERVICE	
SMSvcHost.exe	3296	v4.0.30319	NETWORK SERVICE	-NetMsmqActivator
snmp.exe	2920	System32	SYSTEM	
spoolsv.exe	2688	System32	SYSTEM	
svchost.exe	780	system32	SYSTEM	-k DcomLaunch
svchost.exe	836	system32	NETWORK SERVICE	-k RPCSS
svchost.exe	936	System32	NETWORK SERVICE	-k termsvcs
svchost.exe	988	System32	LOCAL SERVICE	-k LocalServiceNetworkRestricted
svchost.exe	996	system32	LOCAL SERVICE	-k LocalService
svchost.exe	76	System32	SYSTEM	-k LocalSystemNetworkRestricted
svchost.exe	392	system32	NETWORK SERVICE	-k NetworkService
svchost.exe	880	system32	SYSTEM	-k ICService

Finally, click on the **Connections** tab. After selecting a specific connection, **right-click** and choose **Kill Connection** to terminate the communication between the victim machine and the associated port

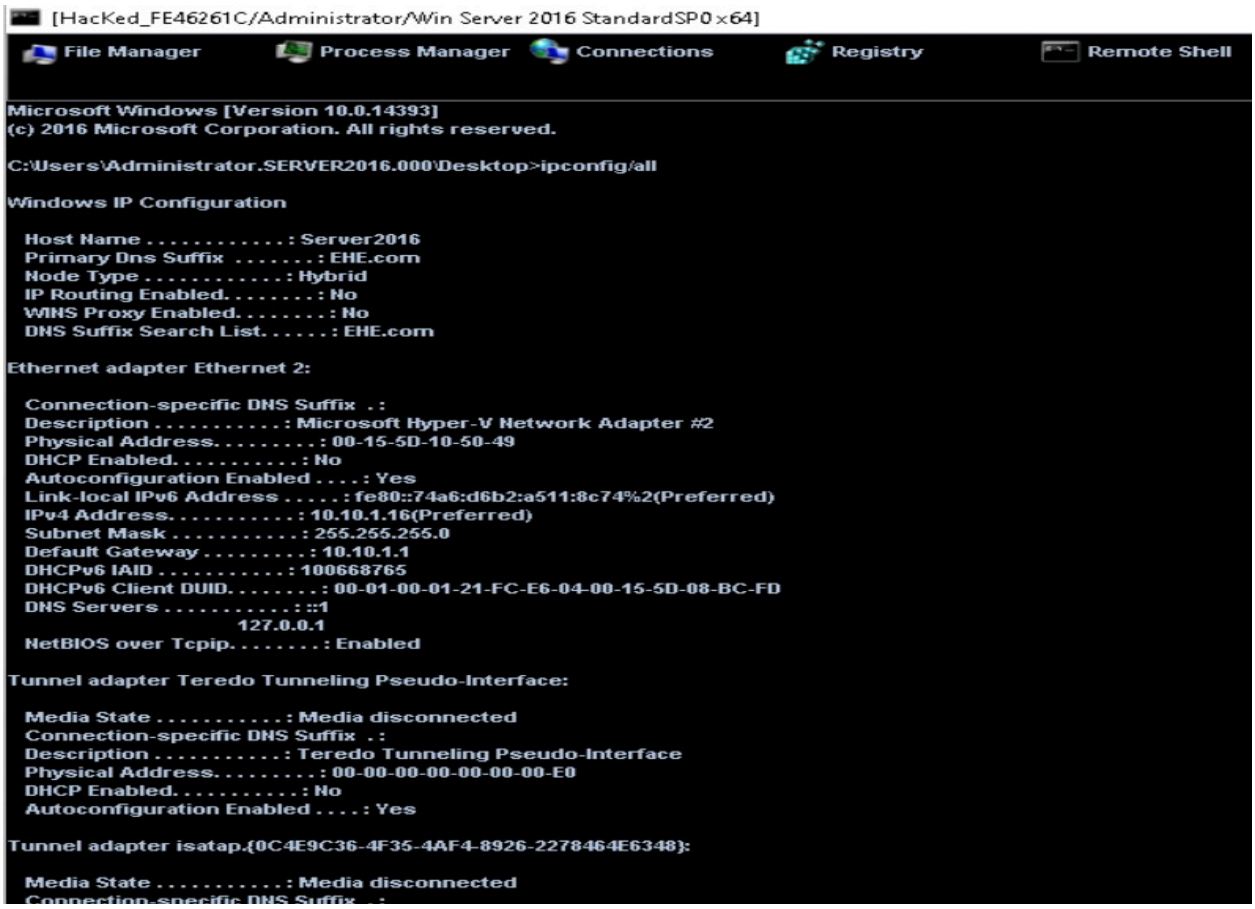
Click the registry tab,



Click Remote Shell. This launches a remote command prompt for the victim machine Type the command ipconfig/all and press Enter.

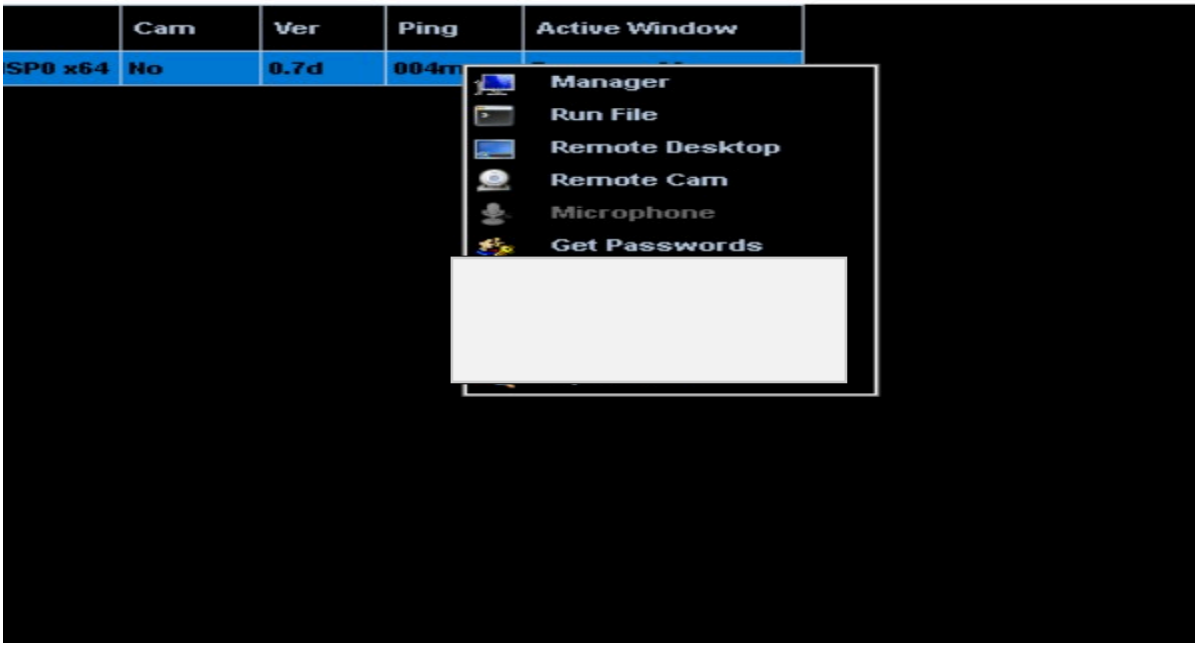


This displays all interfaces related to the victim machine,



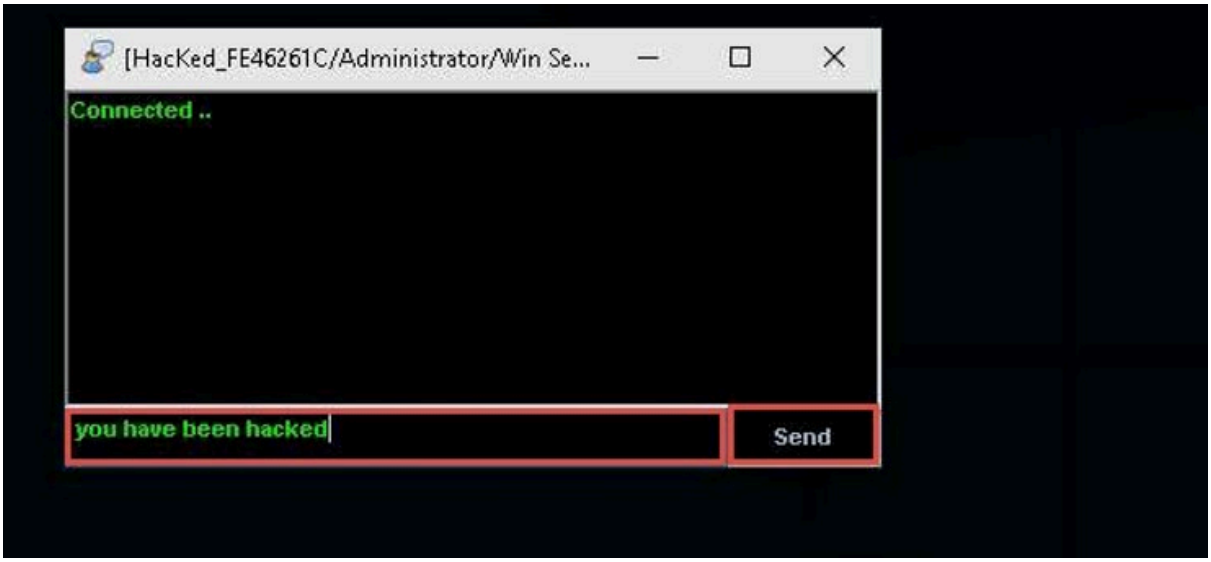
Now, Close the Manager window

Right-click on the victim name, and click Open Chat

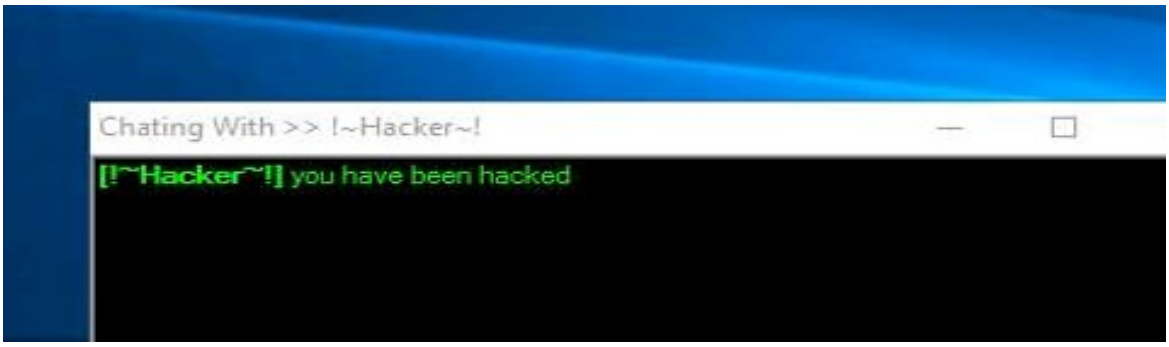


A Chat pop-up appears; enter a nickname (here, Hacker) and click OK

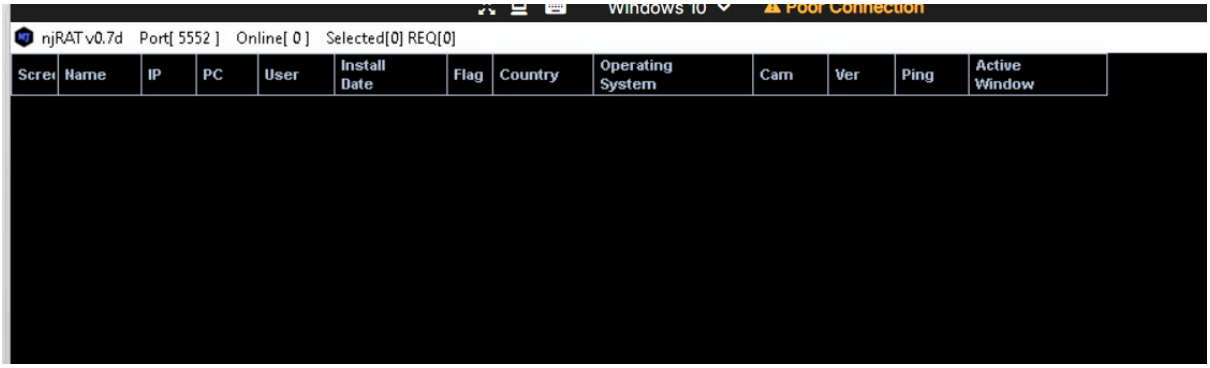
A chat box appears; type a message, and then click Send



In Victim's Machine,



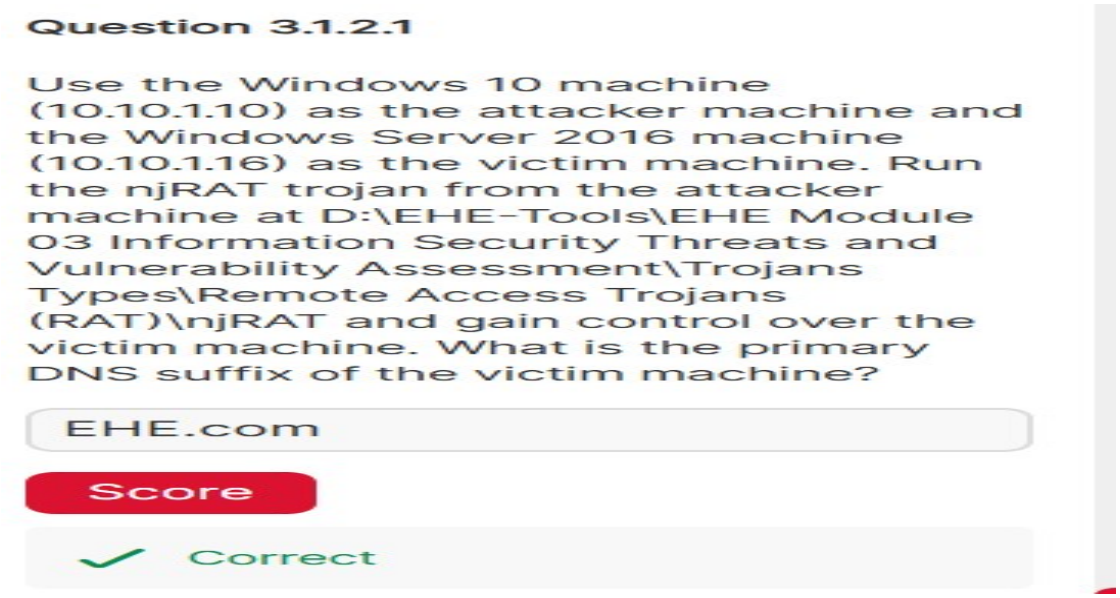
If the victim shut down the system , njRAT loses its connection with Windows Server 2016(victim)



njRAT is designed to automatically establish a connection once the victim logs in. After the malicious file is executed and the system restarts or the user logs back in, the **attacker's client (njRAT)** automatically detects and connects to the victim machine — no manual re-connection is needed

On completion of this lab, click Windows Server 2016 to switch to the **Windows Server 2016** machine, launch **Task Manager**, look for the **server.exe (32 bit)** process

QUIZ:



Ethical Hacking Lab Report – 06 (Date: 05-05-2025)

EC-Council Lab Assignment: Module 4

Password Cracking Techniques and Countermeasures

Objective

- This lab is about understanding how passwords can be cracked. Password cracking means figuring out a password using different methods, like guessing or using special tools. People might crack passwords to recover their own lost passwords, check if a system is secure, or—unfortunately—break into systems without permission.
- In this lab, you will see how weaknesses in security can be exploited and how different password-cracking techniques work. The main goal is to learn how to monitor a system remotely and understand how someone might bypass security controls to gain access.
- It's important to use this knowledge responsibly—to strengthen security, not to break it! Let me know if you need a clearer explanation or more details.